数理解析研究所講究録 1256 巻 2002 年 131-160

Geometrical Structure and Number Theory on Supersingular Loci with Endomorphism Structure

東京大学数理科学研究科 博士 2 年 原下 秀士 (Shushi Harashita)
Graduate School of Mathematical Sciences, The University of Tokyo.

Abstract

This manuscript consists of two parts. At first, we introduce a minimum set of the recent developments on the structure on the moduli space of abelian varieties over fields of positive characteristic. Next we explain an analysis of the structure of the moduli space of supersingular abelian varieties with endomorphism structure.

0 Introduction

Our main subjects are to investigate the relations between the geometry on the moduli spaces $\mathcal{A}_{g,d,n}$ of polarized abelian varieties constructed in [17] or their variants and the arithmetic of some algebraic groups.

It has been important to investigate how we can write the geometical structure on $\mathcal{A}_{g,d,n}$ in terms of the arithmetic of some algebraic groups. Many subjects in attempts to prove Langlands' conjecture may be in this category in a certain sense. On supersingular loci, we already know various beautiful connections between the geometry on the space and arithmetic of quaternion unitary groups. We shall give detailed accounts hereinafter. Conversely we expect that geometrical arguments make it possible to investigate the number theoretic problems on $\mathcal{A}_{g,d,n}$ intuitively.

On the geometrical side, we have two important structures on $\mathcal{A}_{g,d,n}$. One is a stratification by the isogeny classes, which has been investigated since many years ago. The other one was introduced by F. Oort and T. Ekedahl recently, called Ekedahl-Oort stratification, which is defined by the polarization types on p-torsion points of abelian varieties.

In §1, we review such stratifications and state known results. At the last of §1, we shall describe some prospects (philosophy ?). In §2, we explain the structure of the moduli space $S_{g,L}$ of principally polarized supersingular abelian varieties with endomorphism structure of algebraic number field L. Finally I announce that there were many mistakes in my speech and apologize for that.

1 Background and known results

1.1 Isogeny classes

We fix a rational prime p once and for all throughout this paper. Take a perfect field K of characteristic p. Let X be an abelian variety over K. Then we have p-divisible group $\varphi_p(X) = \varinjlim X[p^i]$. We set

$$A_K = W(K)[F,V]/(FV-p, VF-p, Fa = a^\tau F, Va = a^{\tau^{-1}}V, \forall a \in W(K)),$$

with the Frobenius τ over $\mathbb{F}_p$. We define A to be a p-adic completion of A_K. Dieudonné module is a left A-module finitely generated as $W(K)$-module. If a Dieudonné moduli is free as $W(K)$-module, we call it free. There is a functor called Dieudonné functor $\mathbb{D}$ from the category of p-divisible groups to the category of free Dieudonné modules. Then the Dieudonné module $\mathbb{D}(X) := \mathbb{D}(\varphi_p(X))$ has to be isogenous to one of the following forms:

$$(A_{1,0} \oplus A_{0,1})^{\oplus f} \oplus \bigoplus_{(m,n)=1} (A_{m,n} \oplus A_{n,m}) \oplus A_{1,1}^{\oplus s}, \qquad (1)$$

with $A_{m,n} = A/(F^m - V^n)$.

Definition 1.1 *Let X be an abelian variety of dimension g. Assume $g \geq 2$. X is called supersingular (resp. superspecial) if the following equivalent conditions are satisfied:*

1. *X is isogenous (resp. isomorphic) to E^g for a certain supersingular elliptic curve E,*
2. *$\mathbb{D}(X)$ is isogeous (resp. isomorphic) to $A_{1,1}^{\oplus g}$.*

For an abelian variety X, we get a concave line graph, called Newton polygon, from $(0,0)$ to $(2g,g)$ in $\mathbb{R}\times\mathbb{R}$ by drawing vectors $(m+n,n)$ for every component $A_{m,n}$ of $\mathbb{D}(X)$ which is supposed to be isogenous to the form (1).

For each Newton polygon β, we can define the closed subscheme W_β of $\mathcal{A}_{g,1,1}$ which parametrizes abelian varieties with Newton polygon above β. On the dimension of the strata W_β, F. Oort proved in [22]:

Theorem 1.2 *For each Newton polygon β, the dimension of each irreducible component of W_β is equal to $\sharp\Delta(\beta)$, where*

$$\Delta(\beta) = \{(x,y) \in \mathbb{Z}\times\mathbb{Z} \mid y < g, y < x \leq g, (x,y) \text{ is above } \beta\}.$$

Furthermore, T. Ekedahl and F. Oort showed the connectedness of W_β in [4].

F. Oort conjectures that if W_β is not a supersingular locus S_g, then W_β is irreducible.

1.2 Ekedahl-Oort stratification

Every aspects in this subsection was exploited by F. Oort and his colleagues. Please see [23] and so on for detailed arguments. Let X be a principally polarized abelian variety over field of charactristic p. We denote by W the set of words generated by V and F^{-1}. We can show that there is a filtration of $X[p]$:

$$0 = N_0 \subset N_1 \subset \cdots \subset N_r \subset \cdots \subset N_{2r} = X[p]$$

such that $\{N_i\} = \{wX[p] | w \in W\}$. We define $\nu : \{1, 2, \cdots, 2r\} \to \{1, 2, \cdots, r\}$ by $VN_i = N_{\nu(i)}$ and $\rho : \{1, 2, \cdots, 2r\} \to \{1, 2, \cdots, 2g\}$ by $\operatorname{rk} N_i = p^{\rho(i)}$. From the above filtration, we construct the sequence:

$$\varphi = (\varphi(1), \varphi(2), \cdots, \varphi(g))$$

with $\varphi(0) = 0$, satisfying $\varphi(i) \leq \varphi(i+1) \leq \varphi(i) + 1$ by

$$\varphi(\rho(i)) = \varphi(\rho(i) + 1) = \cdots = \varphi(\rho(i+1))$$

if $v(i) = v(i+1)$ and

$$\varphi(\rho(i)) < \varphi(\rho(i) + 1) < \cdots < \varphi(\rho(i+1))$$

if $v(i) < v(i+1)$. A sequence $\varphi = (\varphi(1), \varphi(2), \cdots, \varphi(g))$ is said to be an elementary sequence if it satisfies $\varphi(i) \leq \varphi(i+1) \leq \varphi(i) + 1$.

Set $|\varphi| = \sum_{i=1}^{g} \varphi(i)$.

We denote by S_φ the locally closed subscheme of $\mathcal{A}_{g,1,n}$ which parametrizing the abelian varieties with elementary sequence φ.

The a-number of an abelian variety X over a perfect field K of characteristic p is defined as

$$a(X) = \dim_K(\alpha_p, X),$$

where α_p is the kernel of the Frobenius map $F : \mathbb{G}_a \to \mathbb{G}_a$. It is checked that $a(X)$ is equal to $g - \varphi(g)$ if X is in $S_\varphi(K)$.

We denote by $T_{a,n}$ the closed subscheme of $\mathcal{A}_{g,1,n}$ consisting of abelian varieties of a-number $\geq a$.

F. Oort has proved

Theorem 1.3 *1. S_φ is quasi-affine.*

2. $\dim S_\varphi = |\varphi|$.

3. $\mathcal{A}_{g,1,n} = \coprod_\varphi S_\varphi$ and $S_\varphi \neq \emptyset$ for all elementary sequences φ.

4. We denote by ∂S_φ the boundary $S_\varphi^c - S_\varphi$ in $\mathcal{A}_{g,1,n}$, we have

$$\partial S_\varphi = \coprod_{\varphi'} S_{\varphi'}$$

the union taken over all φ' such that $\varphi' \neq \varphi$ and $S_\varphi^c \cap S_{\varphi'} \neq \emptyset$.

5. $S^c_{\{0,0,\cdots,0,1\}}$ *is connected and contained in* $S_g \cap T_{g-1,n}$.

6. *Non ordinary locus* $T_{1,n} = \mathcal{A}_{g,1,n} - S_{\{1,2,\cdots,g\}}$ *is geometically irreducible.*

In [5], G. van der Geer obtained a generalization of 6 in the above theorem:

Theorem 1.4 *For any* $a < g$, *the locus* $T_{a,1}$ *is irreducible.*

1.3 Supersingular loci

In the book [16], K.-Z Li and F. Oort investigate the supersingular locus S_g. The main theorem says

Theorem 1.5 *There is a quasi-finite surjective morphism defined over* $\mathbb{F}_{p^2}$

$$\Psi : \coprod_{\eta \in \Lambda} \mathcal{P}'_{g,\eta} \to S_g$$

where Λ *is the set of isomorphism classes of polarization* η *on a superspecial abelian varieties* E^g *satisfying* $\ker \eta = E^g[F^{g-1}]$ *and* $\mathcal{P}'_{g,\eta}$ *is the moduli space of some filtrations of supersingular Dieudonné modules.* $\mathcal{P}'_{g,\eta}$ *is a smooth irreducible variety defined over* $\mathbb{F}_{p^2}$ *of dimension* $\left[\frac{g^2}{4}\right]$.

If we substitute $\mathbb{Q}$ for L in §2, we will get precise definitions and an outline of the proof. Because we shall show analogous results in case with endomorphism structure in §2. As for supersingular locus, we already obtain some relations between the geometry and the arithmetic of some algebraic groups:

1. the number of irreducible components of S_g which equals $\sharp\Lambda$ is equal to the class number of a certain quaternion unitary group;

2. the sum of reciprocals of the degrees of the maps from $\mathcal{P}'_{g,\eta}$ to irreducible components of S_g is equals to the mass which is calculated by the mass formula;

3. the problem on the field ($\mathbb{F}_p$ or $\mathbb{F}_{p^2}$) of definition of each irreducible component is translated into that of Hecke operator of the same group. The number of irreducible components defined over $\mathbb{F}_p$ is written by class number and type number [11].

T. Ibukiyama and K. Hashimoto completely calculated the class number in case $g = 2$ in [7]. Moreover T. Ibukiyama completely classifies finite groups G such that G devides $\mathcal{P}'_{g,\eta}$ and $\mathcal{P}'_{g,\eta}/G$ is the normalization of an irreducible component in [10]. At the same time, he calculated the number of irreducible components with each finite group above. Such results are obtained purely by the calculus of algebraic groups.

1.4 Some prospects

We expect that following three subjects are closely related and each relation can be written down in terms of some algebraic groups:

1. the analysis of the singularities on S_g
2. the determination of the structure of $S_g \cap S_\varphi$
3. the explicit calculation of the number of rational points on S_g.

We have a strategy to resolve such questions, although we can not explain it in detail now. The fundamental idea is to find good division of S_g and analyze each fragment. There are some steps which are difficult without level structure. Therefore I think deep investigations on these problems should be number theoretic.

Since we had one result in the way of these studies, we introduce it below. It seems to be new. Let $S_g(a)$ be the moduli space of principally polarized supersingular abelian varieties with a-number greater than or equal to a, i.e., $S_g(a) = S_g \cap T_{a,1}$. Then we have

$$\dim S_g(a) = \left[\frac{g^2 - a^2 + 1}{4}\right].$$

In the book [16], they have calculated the dimensions for $a = 1, 2, g-1$. In case $a = g$, it is a well-known fact (note that X is superspecial iff $a(X) = g$). Since $a(X) = g - \varphi(g)$, I think this observation is the first step to investigate the above problems.

2 Moduli of supersingular abelian varieties with endomorphism structure

We fix an algebraic number field L with involution $*$ once and for all throughout this paper.. Take a prime ideal $\mathfrak{p}$ in the integer ring $\mathcal{O}_L$ of L lying over p. Let $L_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of L and $\mathcal{O}_\mathfrak{p}$ the ring of integers in $L_\mathfrak{p}$. $d_\mathfrak{p}$ denotes the degree of the extension $L_\mathfrak{p}$ over $\mathbb{Q}_p$, $f_\mathfrak{p}$ the relative degree and $e_\mathfrak{p}$ the ramification index. If $L/\mathbb{Q}$ is a Galois extension, then $d_\mathfrak{p}, f_\mathfrak{p}$ and $e_\mathfrak{p}$ are independent of the choice of $\mathfrak{p}$. Then we frequently abbreviate these to d, e and f. We fix a uniformizer π of $\mathcal{O}_\mathfrak{p}$. Let k be the residue field of $\mathcal{O}_\mathfrak{p}$ and q the cardinal number of k. For a field K containing k, we denote by σ the Frobenius map of K over k and by $\mathcal{O}_\mathfrak{P}$ the unramified extension of $\mathcal{O}_\mathfrak{p}$ with residue field K, i.e., $W(K) \otimes_{W(k)} \mathcal{O}_\mathfrak{p}$. For any group scheme G with a left $\mathcal{O}_\mathfrak{p}$ (resp. $\mathcal{O}_L$)-action θ and for any ideal $\mathfrak{a}$ of $\mathcal{O}_\mathfrak{p}$ (resp. $\mathcal{O}_L$), we set

$$G[\mathfrak{a}] = \bigcap_{a \in \mathfrak{a}} \mathrm{Ker}(\theta(a) : G \to G). \tag{2}$$

Definition 2.1 *A $\mathfrak{p}$-divisible group G over K* consists of a system of finite group schemes $\{G_i\}_{i\in\mathbb{N}}$ over K with left $\mathcal{O}_\mathfrak{p}$-action θ and $\mathcal{O}_\mathfrak{p}$-linear homomorphisms $\iota : G_i \to G_{i+1}$ satisfying

(i) $\mathfrak{p} := \theta(\pi) : G_{i+1} \to G_i$ is surjective, and

(ii) $\iota : G_i \to G_{i+1}[\mathfrak{p}^i]$ is an isomorphism for any i.

We set

$$A_K = \mathcal{O}_\mathfrak{P}[\mathfrak{f}, \mathfrak{v}]/(\mathfrak{f}\mathfrak{v} - q, \mathfrak{v}\mathfrak{f} - q, \mathfrak{f}a - a^\sigma \mathfrak{f}, \mathfrak{v}a - a^{\sigma^{-1}}\mathfrak{v},\ \forall a \in \mathcal{O}_\mathfrak{P}) \tag{3}$$

and

$$A_\mathfrak{P} = \varprojlim A_K/\mathfrak{p}^i A_K. \tag{4}$$

Definition 2.2 *A Dieudonné $\mathcal{O}_\mathfrak{P}$-module* is a left $A_\mathfrak{P}$-module M finitely generated as $\mathcal{O}_\mathfrak{P}$-module. If M is free as $\mathcal{O}_\mathfrak{P}$-module, we call M *free.*

Definition 2.3 Let M be a Dieudonné $\mathcal{O}_\mathfrak{P}$-module. *The dual Dieudonné $\mathcal{O}_\mathfrak{P}$-module M^t* is defined by $\mathrm{Hom}_{\mathcal{O}_\mathfrak{P}}(M, \mathcal{O}_\mathfrak{P})$ with actions of $\mathfrak{f}$ and $\mathfrak{v}$:

$$(\mathfrak{f}\psi)(x) = \psi(\mathfrak{v}x)^\sigma, \quad (\mathfrak{v}\psi)(x) = \psi(\mathfrak{f}x)^{\sigma^{-1}} \tag{5}$$

for any $\psi \in \mathrm{Hom}_{\mathcal{O}_\mathfrak{P}}(M, \mathcal{O}_\mathfrak{P})$ and $x \in M$. We also define *the Cartier dual M^D* of a Dieudonné $\mathcal{O}_\mathfrak{P}$-module M by $\mathrm{Hom}_{\mathcal{O}_\mathfrak{P}}(M, \mathrm{frac}\,(\mathcal{O}_\mathfrak{P})/\mathcal{O}_\mathfrak{P})$ with actions of $\mathfrak{f}$ and $\mathfrak{v}$ as above.

Suppose K is perfect. We introduce a contravariant functor $\mathbb{D}_\mathfrak{p}$ which is called Dieudonné functor from the category of $\mathfrak{p}$-divisible groups over K to that of free Dieudonné $\mathcal{O}_\mathfrak{P}$-modules over K.

Definition 2.4 *Dieudonné functor* $\mathbb{D}_\mathfrak{p}$ is a contravariant functor from the category of $\mathfrak{p}$-divisible groups over K to that of free Dieudonné $\mathcal{O}_\mathfrak{P}$-modules over K defined as follows. Let $G = \{G_i\}$ be a $\mathfrak{p}$-divisible group over K. Then G_i is decomposed into the infinitesimal part G_i^{inf} and the étale part $G_i^{\mathrm{\acute{e}t}}$ [1, p.34]. Put $M(G_i^{\mathrm{inf}}) = \mathrm{Hom}_{\mathcal{O}_\mathfrak{p}}(G_i^{\mathrm{inf}}, \mathcal{O}_\mathfrak{P})$ and $M(G_i^{\mathrm{\acute{e}t}}) = M((G_i^{\mathrm{\acute{e}t}})^D)^t$. Here $\mathrm{Hom}_{\mathcal{O}_\mathfrak{p}}(-,-)$ means the set of $\mathcal{O}_\mathfrak{p}$-linear homomorphisms defined over K between commutative formal groups over K. It has a canonical Dieudonné $\mathcal{O}_\mathfrak{P}$-module structure. The functor $\mathbb{D}_\mathfrak{p}$ is the limit of M.

In the same way as [1, Theorem (Manin) p.85], we obtain

Proposition 2.5 *Assume $K = \overline{K}$. Every Dieudonné $\mathcal{O}_\mathfrak{P}$-module is isogenous to a direct sum of $\{A_\lambda\}$, $\lambda = s/r$, $(r, s) = 1$, $r \geq 1$ with $A_\lambda = A_\mathfrak{P}/(\mathfrak{f}^r - \pi^s, \mathfrak{v}^r - \pi^{rd-s})$. Furthermore, A_λ is free if and only if $0 \leq \lambda \leq d$. We call λ the slope*

Definition 2.6 Let K be an arbitrary field. A free Dieudonné $\mathcal{O}_{\mathfrak{P}}$-module M is called *supersingular* (resp. *superspecial*) if M is isogenous (resp. isomorphic) to $A_{d/2}^{\oplus g}$ over $\overline{K}$ for some g. We call g the genus of M.

An abelian variety over K with endomorphism structure is an abelian variety X over K with $\mathcal{O}_L$-action $\theta : \mathcal{O}_L \to \mathrm{End}_K X$. Let $\varphi_{\mathfrak{p}}(X) := \varinjlim X[\mathfrak{p}^i]$ be the $\mathfrak{p}$-divisible group over K and $\mathbb{D}_{\mathfrak{p}}(X) := \mathbb{D}_{\mathfrak{p}}(\varphi_{\mathfrak{p}}(X))$ the Dieudonné $\mathcal{O}_{\mathfrak{P}}$-module associated to X. We define the isogeny class of X by determining which class in Proposition 2.5 $\mathbb{D}_{\mathfrak{p}}(X)$ belongs to for each $\mathfrak{p}$ lying over p. We can easily check that the following p-adic analogue of Tate's theorem [28] holds: if K is a finite field,

$$\mathrm{Hom}_{\mathcal{O}_L}(X, Y) \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \bigoplus_{\mathfrak{p}} \mathrm{Hom}_{A_{\mathfrak{P}}}(\mathbb{D}_{\mathfrak{p}}(Y), \mathbb{D}_{\mathfrak{p}}(X)) \tag{6}$$

for any two abelian varieties X and Y over K. Refer to [29, p.525], for example. Therefore, the above definition of isogeny classes is equivalent to the usual one if K is finite.

Definition 2.7 Let X be an abelian variety over K with endomorphism structure. We say X is *supersingular* (resp. *superspecial*) at $\mathfrak{p}$ if $\mathbb{D}_{\mathfrak{p}}(X)$ is so. And X is called *supersingular* (resp. *superspecial*) if X is so at every $\mathfrak{p}$ lying over p.

Remark 2.8 The notion of supersingularity is equivalent to the usual one, i.e., X is isogenous to the product of supersingular elliptic curves over an algebraically closed field.

Let I_1 (resp. I_2) be the set of the primes $\mathfrak{p}$ stable under the involution $*$ (resp. the set of representatives of the quotient by the action $*$ of the primes $\mathfrak{p}$ unstable under the involution $*$). Set r_i the number of I_i, then $r_1 + 2r_2$ is the number of the whole of the prime ideals of L lying over p.

$\mathbb{D}_{\mathfrak{p}}(X)$ (resp. $\mathbb{D}_{\mathfrak{p}}(X) \oplus \mathbb{D}_{\mathfrak{p}^*}(X)$) has the Manin symmetry condition for $\mathfrak{p} \in I_1$ (resp. $\mathfrak{p} \in I_2$), i.e., $\mathbb{D}_{\mathfrak{p}}(X)$ (resp. $\mathbb{D}_{\mathfrak{p}}(X) \oplus \mathbb{D}_{\mathfrak{p}^*}(X)$) is isogenous to the following form

$$\bigoplus (A_\lambda \oplus A_{d_{\mathfrak{p}} - \lambda}) \oplus (A_{d_{\mathfrak{p}}/2})^{\oplus s}. \tag{7}$$

For an abelian variety with endomorphism structure, we are able to draw $r_1 + r_2$ pictures of Newton polygons of Dieudonné $\mathcal{O}_{\mathfrak{P}}$-modules. We denote by X^t the dual abelian variety of X and define the endomorphism structure on X^t by $\theta(z^*)^t$. If we write X^t, it is supposed to have this endomorphism structure.

Proposition 2.9 $\mathbb{D}_{\mathfrak{p}}(X)^t \simeq \mathbb{D}_{\mathfrak{p}^*}(X^t)$.

Definition 2.10 *A polarization on* (X, θ) is a polarization $\eta : X \to X^t$ satisfying $\theta(z^*) = \eta^{-1} \circ \theta(z)^t \circ \eta$ for all $z \in \mathcal{O}_L$. In other words, a polarization on (X, θ) is an $\mathcal{O}_L$-linear polarization on X.

Let us translate the notion of polarization on (X, θ) to that of quasi-polarization on $\mathbb{D}_{\mathfrak{p}}(X)$. For each $\mathfrak{p}$, a polarization η on (X, θ) induces homomorphism $\varphi_{\mathfrak{p}}(\eta) : \varphi_{\mathfrak{p}}(X) \to \varphi_{\mathfrak{p}}(X^t)$, which induces the homomorphism $\mathbb{D}_{\mathfrak{p}}(\eta) : \mathbb{D}_{\mathfrak{p}}(X^t) \to \mathbb{D}_{\mathfrak{p}}(X)$. Let $\langle , \rangle_{\mathfrak{p},\eta}$ be the image of $\mathbb{D}_{\mathfrak{p}}(\eta)$ by the injection

$$\mathrm{Hom}_{A_{\mathfrak{P}}}(\mathbb{D}_{\mathfrak{p}}(X^t), \mathbb{D}_{\mathfrak{p}}(X)) \hookrightarrow \mathrm{Hom}_{\mathcal{O}_{\mathfrak{P}}}(\mathbb{D}_{\mathfrak{p}}(X^t) \otimes_{\mathcal{O}_{\mathfrak{P}}} \mathbb{D}_{\mathfrak{p}^*}(X^t), \mathcal{O}_{\mathfrak{P}}). \tag{8}$$

Then the quasi-polarizations $\langle , \rangle_{\mathfrak{p},\eta}$ and $\langle , \rangle_{\mathfrak{p}^*,\eta}$ satisfy the nontrivial relation given by the identity (ii) of the following proposition.

Proposition 2.11 *The $\mathcal{O}_{\mathfrak{P}}$-bilinear form $\langle , \rangle_{\mathfrak{p},\eta}$ induced by a polarization η on (X, θ) is non-degenerate and satisfies*

(i) $\langle \mathfrak{f}x, y\rangle_{\mathfrak{p},\eta} = \langle x, \mathfrak{v}y\rangle^{\sigma}_{\mathfrak{p},\eta}, \quad \langle \mathfrak{v}x, y\rangle_{\mathfrak{p},\eta} = \langle x, \mathfrak{f}y\rangle^{\sigma^{-1}}_{\mathfrak{p},\eta}$,

(ii) $\langle x, y\rangle_{\mathfrak{p},\eta} = -\langle y, x\rangle_{\mathfrak{p}^*,\eta}$.

Given a field K of characteristic p, let $\mathcal{S}_{n,L}(K)$ be the category of supersingular abelian varieties over K with endomorphism structure and $\mathcal{S}_{n,L}(K) \otimes \mathbb{Z}_p$ the category with the same objects as $\mathcal{S}_{n,L}(K)$ and the morphisms defined by $\mathrm{Hom}_L(Y, X) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for $X, Y \in \mathrm{Ob}(\mathcal{S}_{n,L}(K) \otimes \mathbb{Z}_p)$. In this section, we suppose K is an algebraically closed field. For an abelian variety X over K of dimension n, the cup product induces the trace map

$$\mathrm{tr} : \wedge^{2n} H^1_{crys}(X/W(K)) \simeq W(K)[-n]. \tag{9}$$

A. Ogus proved the following result, which he called Torelli's theorem (Theorem 6.2 and Lemma 6.4 in [21]).

Theorem 2.12 *Assume $n \geq 2$. The functor $(\mathbb{D}, \mathrm{tr})$ gives a bijection between the set of isomorphism classes of $\mathcal{S}_{n,\mathbb{Q}}(K)$ and of supersingular Dieudonné modules of genus n with trace map. Besides, for two objects X, Y of $\mathcal{S}_{n,\mathbb{Q}}(K)$, we have*

$$\mathrm{Hom}(X, Y) \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \mathrm{Hom}_A(\mathbb{D}(Y), \mathbb{D}(X)). \tag{10}$$

We remark that this theorem gives an anti-equivalence between $\mathcal{S}_{n,\mathbb{Q}}(K) \otimes \mathbb{Z}_p$ and the category of supersingular Dieudonné modules of genus n without trace map if $n \geq 2$.

The purpose of this section is to show an analogue in case with endomorphism structure. Let X be an object of $\mathcal{S}_{n,L}(K)$. By the above theorem, we obtain the injection $\theta : \mathcal{O}_L \otimes \mathbb{Z}_p \to \mathrm{End}_A \mathbb{D}(X)$. Using $\mathcal{O}_L \otimes \mathbb{Z}_p = \oplus_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}} e_{\mathfrak{p}}$ with idempotents $e_{\mathfrak{p}}$, we get the decomposition

$$\mathbb{D}(X) = \bigoplus_{\mathfrak{p}} \mathbb{D}(X)_{\mathfrak{p}} \tag{11}$$

with $\mathbb{D}(X)_{\mathfrak{p}} = e_{\mathfrak{p}} \mathbb{D}(X)$. Since the $\mathcal{O}_L$-action commutes with A, $\mathbb{D}(X)_{\mathfrak{p}}$ becomes a Dieudonné module. Moreover, $\mathbb{D}(X)_{\mathfrak{p}}$ has to be supersingular. By the above theorem, X is decomposed as $\prod_{\mathfrak{p}} X_{\mathfrak{p}}$ such that $\mathbb{D}(X_{\mathfrak{p}}) \simeq \mathbb{D}(X)_{\mathfrak{p}}$. Since $\mathbb{D}(X_{\mathfrak{p}})$ has a left $\mathcal{O}_{\mathfrak{p}}$-action, we get a Dieudonné $\mathcal{O}_{\mathfrak{P}}$-module $\mathbb{D}_{\mathfrak{p}}(X_{\mathfrak{p}})$. $\mathbb{D}_{\mathfrak{p}}(X_{\mathfrak{p}})$ is not other than $\mathbb{D}_{\mathfrak{p}}(X)$ constructed as above. Set

$$\mathfrak{n} = \frac{n}{r_1 + 2r_2}. \tag{12}$$

Then $\dim X_{\mathfrak{p}} = \mathfrak{n}$ for all $\mathfrak{p}$.

There exists a trace map $\mathrm{tr}_{\mathfrak{p}}$ completing the following diagram

$$\begin{array}{ccccc} \mathrm{End}_{A_{\mathfrak{P}}} \mathbb{D}_p(X_{\mathfrak{p}}) & \xrightarrow{\nu_{\mathfrak{p}}} & \bigwedge^{\frac{2\mathfrak{n}}{d_{\mathfrak{p}}}} \mathbb{D}_{\mathfrak{p}}(X_{\mathfrak{p}}) & \underset{\simeq}{\xrightarrow{\mathrm{tr}_{\mathfrak{p}}}} & \mathcal{O}_{\mathfrak{P}} \\ \downarrow & & \downarrow & & \downarrow N_{L_{\mathfrak{p}}/\mathbb{Q}_p} \\ \mathrm{End}_A \mathbb{D}(X) & \xrightarrow{\nu} & \bigwedge^{2\mathfrak{n}} \mathbb{D}(X_{\mathfrak{p}}) & \underset{\simeq}{\xrightarrow{\mathrm{tr}}} & W(K). \end{array} \tag{13}$$

where $\nu_{\mathfrak{p}}$ and ν are the reduced norms.

Let $g_{\mathfrak{p}} = \mathfrak{n}/d_{\mathfrak{p}}$ (resp. $2\mathfrak{n}/d_{\mathfrak{p}}$) if $d_{\mathfrak{p}}$ is odd (resp. even).

Theorem 2.13 *Suppose $g_{\mathfrak{p}} \geq 2$. The functor $(\mathbb{D}_{\mathfrak{p}}, \mathrm{tr}_{\mathfrak{p}})$ defines the bijection between the set of isomorphism classes of $\{X \in \mathcal{S}_{\mathfrak{n},L}(K) | X = X_{\mathfrak{p}}\}$ and of Dieudonné $\mathcal{O}_{\mathfrak{P}}$-modules of genus $g_{\mathfrak{p}}$ with trac map. Therefore $\oplus_{\mathfrak{p}} \mathbb{D}_{\mathfrak{p}}(-_{\mathfrak{p}})$ gives an anti-equivalence between $\mathcal{S}_{n,L}(K) \otimes \mathbb{Z}_p$ and the category of direct sums of Dieudonné $\mathcal{O}_{\mathfrak{P}}$-modules without trace map, except for $\mathfrak{p}$-components of which $g_{\mathfrak{p}}$ is one.*

Let M be a superspecial Dieudonné $\mathcal{O}_{\mathfrak{P}}$-module. Set $\mathcal{O}'_{\mathfrak{p}} = W(k') \otimes_{W(k)} \mathcal{O}_{\mathfrak{p}}$ with

$$k' = \begin{cases} \text{a quadratic extension over } k & d : \text{odd}, \\ k & d : \text{even}, \end{cases} \tag{14}$$

and if K contains k',

$$H := \mathrm{End}_{A_{\mathfrak{P}}}(A_{d/2}) \simeq \begin{cases} \mathcal{O}'_{\mathfrak{p}}[\mathfrak{f}, \mathfrak{v}]/(\mathfrak{f} - \mathfrak{v}) & d : \text{odd}, \\ \mathcal{O}_{\mathfrak{p}} & d : \text{even}. \end{cases} \tag{15}$$

From now on, K is supposed to contain k'.

When d is odd, there exists a conjugation map $^{-} : H \to H$ sending $a + b\mathfrak{f}$ to $a^{\sigma} - b\mathfrak{f}$. We define the norm map $\mathrm{Nm} : H \to \mathcal{O}_{\mathfrak{p}}$ by $\mathrm{Nm}(x) = \bar{x}x$, which is surjective.

Let us define an H-module attached to M as

$$\tilde{M} = \begin{cases} \{x \in M | (\mathfrak{f} - \mathfrak{v})x = 0\} & d : \text{odd}, \\ \{x \in M | (\mathfrak{f} - \pi^{\frac{d}{2}})x = 0\} & d : \text{even}, \end{cases} \tag{16}$$

which is called the *skeleton* of M. Then $\tilde{M}$ is free as $\mathcal{O}'_{\mathfrak{p}}$-module.

Definition 2.14 *An involution* $*$ *on* $L_{\mathfrak{p}}$ is defined as

(1) the involution naturally induced by the involution $*$ on L for $\mathfrak{p} \in I_1$, and

(2) the trivial one for $\mathfrak{p} \in I_2$.

Lemma 2.15 *A quasi-polarization* $\langle , \rangle_{\mathfrak{p},\eta}$ *on* M *induces a quasi-polarization on* $\tilde{M}$

$$\langle , \rangle_{\mathfrak{p}} : \tilde{M} \otimes_{\mathcal{O}'_{\mathfrak{p}}} \tilde{M} \to \mathcal{O}'_{\mathfrak{p}} \tag{17}$$

satisfying either of the following conditions, depending on the parity of d.

(1) If d is odd,

(i) $\langle , \rangle_{\mathfrak{p}}$ *is an alternating* $\mathcal{O}'_{\mathfrak{p}}$*-bilinear form,*

(ii) $\langle \mathfrak{f}x, y \rangle_{\mathfrak{p}} = \langle x, \mathfrak{v}y \rangle_{\mathfrak{p}}^{\sigma}$, $\langle \mathfrak{v}x, y \rangle_{\mathfrak{p}} = \langle x, \mathfrak{f}y \rangle_{\mathfrak{p}}^{\sigma^{-1}}$.

(2) If d is even, $\langle , \rangle_{\mathfrak{p}}$ *is skew-hermitian, i.e.,* $\langle x, y \rangle_{\mathfrak{p}} = -\langle y, x \rangle_{\mathfrak{p}}^{*}$.

The above pairing $\langle , \rangle_{\mathfrak{p}}$ on $\tilde{M}$ induces a pairing on M:

$$\langle , \rangle_{\mathfrak{p}} : M \otimes M \to \mathcal{O}_{\mathfrak{P}}, \tag{18}$$

by extending $W(K)$-bilinearly. We note that this is a pairing as a $W(K)$-module. For M a quasi-polarized submodule of a quasi-polarized superspecial Dieudonné $\mathcal{O}_{\mathfrak{P}}$-module N, we can define a pairing $\langle , \rangle_{\mathfrak{p}}$ on M, which is $W(K)$-bilinear.

We say $*$ is unramified (resp. ramified), if $L_{\mathfrak{p}}$ is an unramified (resp. ramified) extension over $*$-invariant subfield of $L_{\mathfrak{p}}$.

Proposition 2.16 *Let* $\{M, \langle , \rangle_{\mathfrak{p}}\}$ *be a quasi-polarized superspecial Dieudonné* $\mathcal{O}_{\mathfrak{P}}$*-module. Then we have a decomposition:*

$$M \simeq M_1 \oplus M_2 \oplus \cdots \oplus M_m, \qquad \langle M_i, M_j \rangle_{\mathfrak{p}} = 0, \quad \text{if } \ i \neq j, \tag{19}$$

with indecomposable quasi-polarized Dieudonné $\mathcal{O}_{\mathfrak{P}}$*-modules* M_i*. Here* M_i *are given as follows.*

(1) For odd d, each M_i *is either*

(i) $M_i = A_{\mathfrak{P}}x \simeq A_{d/2}$ *such that* $\langle x, \mathfrak{f}x \rangle_{\mathfrak{p}} = \pi^r \varepsilon$, $\varepsilon^{\sigma} = -\varepsilon \in \mathcal{O}'_{\mathfrak{p}} - \pi\mathcal{O}'_{\mathfrak{p}}$

or

(ii) $M_i = A_{\mathfrak{P}}x \oplus A_{\mathfrak{P}}y \simeq A_{d/2}^{\oplus 2}$ *such that* $\langle x, y \rangle_{\mathfrak{p}} = \pi^r$, $\langle x, \mathfrak{f}x \rangle_{\mathfrak{p}} = \langle y, \mathfrak{f}y \rangle_{\mathfrak{p}} = \langle x, \mathfrak{f}y \rangle_{\mathfrak{p}} = \langle y, \mathfrak{f}x \rangle_{\mathfrak{p}} = 0$.

Here x, y *are in the skelton* $\tilde{M}$.

(2) *For even d and non-trivial $*$, the description of M_i depends on the ramification of $*$:*

(a) *if $*$ is unramified, $M_i = A_{\mathfrak{P}} x \simeq A_{d/2}$ such that $\langle x, x\rangle_{\mathfrak{p}} = \pi^r \varepsilon$, $\varepsilon^* = -\varepsilon \in \mathcal{O}_{\mathfrak{p}} - \pi \mathcal{O}_{\mathfrak{p}}$ $(x \in \tilde{M})$,*

(b) *if $*$ is ramified, $M_i = A_{\mathfrak{P}} x \simeq A_{d/2}$ such that $\langle x, x\rangle_{\mathfrak{p}} = \pi^r \varepsilon$, $\varepsilon^* = \varepsilon \in \mathcal{O}_{\mathfrak{p}} - \pi \mathcal{O}_{\mathfrak{p}}$ $(x \in \tilde{M})$. In this case, r has to be odd.*

(2′) *For even d and trivial $*$, we have $M_i = A_{\mathfrak{P}} x \oplus A_{\mathfrak{P}} y \simeq A_{d/2}^{\oplus 2}$ such that $\langle x, y\rangle_{\mathfrak{p}} = \pi^r$ $(x, y \in \tilde{M})$ for any i.*

Assume K is a perfect field containing k'. Let X be a supersingular abelian variety of dimension n over K with endomorphism structure. Assume $X = X_{\mathfrak{p}}$. Set $g = n/d$ (resp. $2n/d$) if d is odd (resp. even).

Proposition 2.17 *Let X be as above. There exist a superspecial abelian variety Y and $\mathcal{O}_L$-linear isogeny $\varphi : Y \longrightarrow X$ satisfying the following universal property: for any superspecial abelian variety Z and any $\mathcal{O}_L$-linear isogeny $\psi : Z \longrightarrow X$, there is, up to isomorphism, a unique $\mathcal{O}_L$-linear isogeny, $\phi : Z \longrightarrow Y$ such that $\psi = \varphi \circ \phi$.*

This proposition essentially follows from the lemma below. Its proof is similar to that of [16, Lemma 1.8].

Lemma 2.18 *For two superspecial Dieudonné $\mathcal{O}_{\mathfrak{p}}$-modules contained in a certain Dieudonné $\mathcal{O}_{\mathfrak{p}}$-module, their intersection and sum are also superspecial.*

This lemma is an analogy of [15, Lemma 1.3]. We can prove this in the same way.

Notation 2.19 By the above lemma, we have the biggest superspecial Dieudonné $\mathcal{O}_{\mathfrak{P}}$-module $S_0(M)$ contained in M and the smallest one $S^0(M)$ containing M, in $M \otimes_{\mathcal{O}_{\mathfrak{P}}} \operatorname{frac} \mathcal{O}_{\mathfrak{P}}$, for any supersingular Dieudonné $\mathcal{O}_{\mathfrak{P}}$-module M.

Define a left $A_{\mathfrak{P}}$-ideal by

$$I = \begin{cases} (\mathfrak{f}, \mathfrak{v}) & d : \text{odd}, \\ (\mathfrak{f}, \pi^{\frac{d}{2}}, \mathfrak{v}) & d : \text{even}. \end{cases} \tag{20}$$

For convenience, we set

$$q' = \begin{cases} q^2 & d : \text{odd}, \\ q & d : \text{even}. \end{cases} \tag{21}$$

By definition, we have the following proposition.

Proposition 2.20 *We obtain $\mathfrak{f}^{g-1} S(M) = S_0(M)$ and $\mathfrak{f}^{g-1} S^0(M) = S_0'(M)$.*

Remark 2.21 *When d is even, $I^{[\frac{g}{2}]}M$ is superspecial.*

When $*$ is ramified, we denote by $\mathcal{O}_{\mathfrak{p}}{}''$ the unramified quadratic extension of $\mathcal{O}_{\mathfrak{p}}$. In the other cases, we set $\mathcal{O}_{\mathfrak{p}}{}'' = \mathcal{O}_{\mathfrak{p}}$ for convenience. Set

$$R = \begin{cases} \mathcal{O}_{\mathfrak{P}}/\pi^d & d : \text{odd}, \\ \mathcal{O}_{\mathfrak{P}}/\pi^{\frac{d}{2}} & d : \text{even}. \end{cases} \tag{22}$$

Definition 2.22 *A rigid PFTQ over K* is a filtration of quasi-polarized Dieudonné $\mathcal{O}_{\mathfrak{P}}$-modules $\{M_0 \subset M_1 \subset \cdots \subset M_{g-1}\}$ such that

(i) $M_{g-1} \simeq A_{d/2}^{\oplus g}$ and $M_{g-1}^t = \mathfrak{f}^{g-1}M_{g-1}$,

(ii) $IM_i \subset M_{i-1}$ and M_i/M_{i-1} is a free R-module of rank i,

(iii) $I^iM_i \subset M_i^t$,

(iv) $M_i = M_0 + \mathfrak{f}^{g-1-i}M_{g-1}$. The last condition is called rigidity.

Proposition 2.23 *Suppose K is perfect. Assume p is odd. For any principally quasi-polarized supersingular Dieudonné $\mathcal{O}_{\mathfrak{P}}$-module of genus g, there is a rigid PFTQ $\{M_0 \subset M_1 \subset \cdots \subset M_{g-1}\}$ such that $M_0 \simeq M$.*

Proof. We prove this lemma by induction. Set $N = S^0(M)$. There is a superspecial Dieudonné $\mathcal{O}_{\mathfrak{P}}$-module N' of genus 2 such that $N = N' \oplus N''$ and for some superspecial Dieudonné $\mathcal{O}_{\mathfrak{P}}$-module N''' of genus 2 containing N', we have $N'''^t = \pi^n N'''$ ($n < dg$ if d is odd and $2n < dg$ if d is even) and N is not in $\pi N'''$. We can choose the generators x, y of N''' such that

$$\langle x, x\rangle_{\mathfrak{p}} = \langle x, \mathfrak{f}x\rangle_{\mathfrak{p}} = \langle y, y\rangle_{\mathfrak{p}} = \langle y, \mathfrak{f}y\rangle_{\mathfrak{p}} = 0. \tag{23}$$

There is a self-dual complex

$$C^{\cdot} : 0 \to A_{\mathfrak{P}}\pi^n y \to M \to A_{\mathfrak{P}}x \to 0. \tag{24}$$

Since $\langle x, M \cap A_{\mathfrak{P}}y\rangle \in \mathcal{O}_{\mathfrak{P}}$, we get $M \cap A_{\mathfrak{P}}y = A_{\mathfrak{P}}\pi^n y$. Hence $M' = H^1(C^{\cdot})$ is a principally quasi-polarized supersingular Dieudonné $\mathcal{O}_{\mathfrak{P}}$-module of genus $g-2$. By induction, M' has a rigid PFTQ $\{M_0' \subset \cdots \subset M_{g-3}'\}$. Let M_{g-1} be the submodule in $M \otimes_{\mathcal{O}_{\mathfrak{P}}} (\operatorname{frac} \mathcal{O}_{\mathfrak{P}})$ generated by x, $\pi^n\mathfrak{f}^{-g+1}y$ and $\mathfrak{f}^{-1}M_{g-3}'$. Put $M_i = M + \mathfrak{f}^{g-1-i}M_{g-1}$. Then these satisfy all conditions of the definition of rigid PFTQ. ∎

2.1 Moduli of rigid PFTQs

In this section, we investigate a local chart of the moduli space D_g of principally quasi-polarized supersingular Dieudonné $\mathcal{O}_{\mathfrak{P}}$-modules of genus g in the similar way as in [16, Chapter 7].

In the case when d is odd, we can do almost in the same way as in [16]. Let $\mathcal{N}_g$ be the moduli space of all of rigid PFTQs. If d is odd, $\mathcal{N}_g$ is smooth and irreducible, but not so if d is even. In this section, we restrict ourselves to investigating the case that d is even, $*$ is not trivial and p is odd. Let S be a reduced k-scheme. Let $W(\mathcal{O}_S)$ be the sheaf of Witt rings [26]. Set $\mathcal{O}_{\mathfrak{P}} = W(\mathcal{O}_S) \otimes_{W(k)} \mathcal{O}_{\mathfrak{p}}$, $R_S = R \otimes \mathcal{O}_S$ and $A_{\mathfrak{P}} = W(\mathcal{O}_S) \cdot H$. In this section, we abbreviate $M^{(p^i)}$ to M (i.e., for example $\mathfrak{f} : M \to M$ means $\mathfrak{f} : M^{(q)} \to M$) and $\mathcal{O}_{\mathfrak{P}}|_U, A_{\mathfrak{P}}|_U$ to $\mathcal{O}_{\mathfrak{P}}, A_{\mathfrak{P}}$ for any open subscheme U of S. We can define Dieudonné $\mathcal{O}_{\mathfrak{P}}$-modules over S in an analogeous way as in [16, 5.4].

Definition 2.24 *A rigid PFTQ over* S is a filtration $\{M_0 \subset M_1 \subset \cdots \subset M_{g-1}\}$ of Dieudonné $\mathcal{O}_{\mathfrak{P}}$-modules over S such that

(i) $M_{g-1} \simeq A_{d/2}^{\oplus g}$ and $M_{g-1}^t = \mathfrak{f}^{g-1} M_{g-1}$,

(ii) $IM_i \subset M_{i-1}$ and M_i/M_{i-1} is a locally free R_S-module of rank i,

(iii) $I^i M_i \subset M_i^t =: M^i$,

(iv) $M_i = M_0 + \mathfrak{f}^{g-1-i} M_{g-1}$ (rigidity).

Definition 2.25 For a Dieudonné $\mathcal{O}_{\mathfrak{P}}$-module M over K, *the a-number* of M is the length of M/IM, denoted by $a(M)$.

Let $\tilde{\Phi}$ be the set of $H \otimes_{\mathcal{O}_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}}''$-basis $\Theta = \{x_0, x_1, x_2, \ldots, x_{g-2}, x_{g-1}\}$ of $\tilde{M}_{g-1} \otimes_{\mathcal{O}_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}}''$ such that for all i, j, $\langle x_i, \mathfrak{f}^{g-1} x_{g-1-j} \rangle_{\mathfrak{p}} = \varepsilon \delta_{ij}$ with ε as in Proposition 2.16 (2). We call an element of $\tilde{\Phi}$ *a standard basis.*

Definition 2.26 *For a given standard basis* $\Theta = \{x_0, x_1, \cdots, x_{g-1}\}$*,* U^{Θ} *is the set consisting of rigid PFTQs* $\{M_0 \subset \cdots \subset M_{g-1}\}$ *with basis* Θ *of* M_{g-1} *such that* M_0 *has a basis of following type:*

$$w_i = \sum_{j \geq i} \alpha_{ij} \mathfrak{f}^i x_j$$

with $\alpha_{ii} = 1$ *and* $\alpha_{ij} \in A_{\mathfrak{P}}$.

Now we want to show that any rigid PFTQ

$$\mathfrak{M} = \{M_0 \subset \cdots \subset M_{g-1}\}$$

is contained in U^{Θ} for some Θ. This is shown by several steps.

<u>Claim 1</u> : For given $\mathfrak{M}$, there is a basis $\Theta = \{x_0, \cdots, x_{g-1}\} \in \tilde{\Phi}$ such that the natural map $M_0 \to A_{\mathfrak{P}} x_0$ is surjective.

Proof. Let $\{M_0 \subset \cdots \subset M_{g-1}\}$ be a rigid PFTQ. We take a basis $\Theta' = \{x'_0, \cdots, x'_{g-1}\} \in \tilde{\Phi}$. Since $M^0/M^1 \simeq R$ and $M^1 = M^0 \cap \mathfrak{f}M_{g-1}$, there is an element v of M^0 generating M^0/M^1. Then v can be written as

$$v = \gamma_0 x'_0 + \gamma_1 x'_1 + \cdots + \gamma_{g-1} x'_{g-1}$$

and $\gamma_i \notin \pi \mathcal{O}_{\mathfrak{P}}$ for some i.

We define Θ by setting $x_0 = x'_i, x_{g-1} = x'_{g-1-i}, x_i = x'_0, x'_{g-1-i} = x'_{g-1}$ and $x_j = x'_j$ for all $j \neq 0, i, g-1-i, g-1$. By dividing v by γ_i, we have w_0 which generates M^0/M^1 and has x_0-coefficient 1. ▮

<u>Claim 2</u> : For given $\mathfrak{M}$ and a basis $\Theta = \{x_0, \cdots, x_{g-1}\} \in \tilde{\Phi}$ satisfying the condition that the map $M_0 \to A_{\mathfrak{P}} x_0$ is surjective, we can define a derived rigid PFTQ $\overline{\mathfrak{M}}$ of genus $g-2$.

Construction and proof. From the surjection $M_0 \to A_{\mathfrak{P}} x_0$, we have the self-dual complex

$$C_0^{\cdot} : 0 \to A_{\mathfrak{P}} \mathfrak{f}^{g-1} x_{g-1} \to M_0 \to A_{\mathfrak{P}} x_0 \to 0.$$

Since $\langle x_0, M_0 \cap A_{\mathfrak{P}} x_{g-1} \rangle_p \in \mathcal{O}_{\mathfrak{P}}$, we have $M_0 \cap A_{\mathfrak{P}} x_{g-1} = A_{\mathfrak{P}} \mathfrak{f}^{g-1} x_{g-1}$, which implies $M'_0 := H^1(C_0^{\cdot})$ is a principally quasi-polarized supersingular Dieudonné $\mathcal{O}_{\mathfrak{P}}$-module of genus $g-2$. We have also a complex

$$C_{i+1}^{\cdot} : 0 \to A_{\mathfrak{P}} \mathfrak{f}^{g-2-i} x_{g-1} \to M_{i+1} \to A_{\mathfrak{P}} x_0 \to 0.$$

Put $M'_i := H^1(C_{i+1}^{\cdot})$. Note $M'_0 = H^0(C_0^{\cdot}) = H^1(C_1^{\cdot})$. Since $\langle \mathfrak{f}^{i+1} x_0, M_{i+1} \cap A_{\mathfrak{P}} x_{g-1} \rangle_p \in \mathcal{O}_{\mathfrak{P}}$, we have $M_{i+1} \cap A_{\mathfrak{P}} x_{g-1} = (M_0 + \mathfrak{f}^{g-2-i} M_{g-1}) \cap A_{\mathfrak{P}} x_{g-1} = A_{\mathfrak{P}} \mathfrak{f}^{g-2-i} x_{g-1}$. Therefore M'_i is a quasi-polarized supersingular Dieudonné $\mathcal{O}_{\mathfrak{P}}$-module of genus $g-2$.

We show that $\overline{\mathfrak{M}} := \{M'_0 \subset \cdots \subset M'_{g-3}\}$ is a rigid PFTQ of genus $g-2$. First of all, we show that M'_{g-3} is a superspecial. We have $M_{g-2} = M_0 + \mathfrak{f}M_{g-1} = A_{\mathfrak{P}} w_0 + \mathfrak{f}M_{g-1}$, because $M_0/M^1 = R < \overline{w}_0 >$ and $M^1 = M_0 \cap \mathfrak{f}M_{g-1}$. Hence $\ker(M_{g-2} \to A_{\mathfrak{P}} x_0) = \mathfrak{f}M_{g-1}$, so we obtain $M'_{g-3} = A_{\mathfrak{P}} < \mathfrak{f}x_1, \cdots, \mathfrak{f}x_{g-1} >$, which is superspecial. Next, we show that the rigidity: $M'_i = M_0 + \mathfrak{f}^{g-3-i} M'_{g-3}$. In fact,

$$\begin{aligned} M'_i &= \ker(M_{i+1} \to A_{\mathfrak{P}} x_0)/A_{\mathfrak{P}} \mathfrak{f}^{g-2-i} x_{g-1} \\ &= \ker(M_0 + \mathfrak{f}^{g-2-i} M_{g-1} \to x_{g-1})/A_{\mathfrak{P}} \mathfrak{f}^{g-2-i} x_{g-1} \\ &= \ker(M_0 \to A_{\mathfrak{P}} x_0)/M_0 \cap A_{\mathfrak{P}} \mathfrak{f}^{g-2-i} x_{g-1} + \mathfrak{f}^{g-3-i} M'_{g-3} \\ &= M'_0 + \mathfrak{f}^{g-3-i} M'_{g-3}. \end{aligned}$$

The rigidity implies that $IM'_i \subset M'_{i-1}$ and $I^i M'_i \subset M'^i$. Finally $M'_i/M'_{i-1} \simeq R^{\oplus i}$ follows from the exact sequence

$$0 \to H^1(C_i^{\cdot}) \to H^1(C_{i+1}^{\cdot}) \to R^{\oplus i} \to 0$$

induced by the commutative diagram:

$$\begin{array}{cccccccccc}
C_i^{\cdot} & 0 & \longrightarrow & A_{\mathfrak{P}}\mathfrak{f}^{g-1-i}x_{g-1} & \longrightarrow & M_i & \longrightarrow & A_{\mathfrak{P}}x_0 & \longrightarrow & 0 \\
 & & & \downarrow & & \downarrow & & \downarrow & & \\
C_{i+1}^{\cdot} & 0 & \longrightarrow & A_{\mathfrak{P}}F^{g-2-i}x_{g-1} & \longrightarrow & M_{i+1} & \longrightarrow & A_{\mathfrak{P}}x_0 & \longrightarrow & 0 \\
 & & & \downarrow & & \downarrow & & \downarrow & & \\
 & 0 & \longrightarrow & R & \longrightarrow & R^{\oplus i+1} & \longrightarrow & 0 & \longrightarrow & 0. \blacksquare
\end{array}$$

<u>Claim 3</u> : Under the same notation and assumptions as the above claim 2, for an standard basis $\overline{\Theta} = \{\overline{x}_1, \cdots, \overline{x}_{g-2}\}$ of genus $g-2$ such that $\overline{\mathfrak{M}} \in U^{\overline{\Theta}}$, we can construct a basis Θ' of genus g from the data $\mathfrak{M}, \Theta, \overline{\Theta}$ such that $\mathfrak{M} \in \mathfrak{U}^{\Theta'}$.
Construction and proof. By the hypothesis, M_0' is generated by following forms

$$w_i' = \sum_{j=i}^{g-2} \alpha_{ij}' \overline{x}_j \qquad \text{with } \alpha_{i,i}' = 1 \text{ and } \alpha_{ij}' \in A_{\mathfrak{P}} \tag{25}$$

for $i = 1, 2, \cdots, g-2$. Then M_0 is generated by w_0, $\mathfrak{f}^{g-1}x_{g-1}$ and the lifts w_i of w_i'. If we put

$$\Theta = \{x_0, \cdots, x_{g-1}\} := \{x_0, \overline{x}_1, \overline{x}_2, \cdots, \overline{x}_{g-2}, x_{g-1}\} \in \tilde{\Phi},$$

then we can see that M_0 has a basis $\{w_0, w_1, \cdots, w_{g-1}\}$ which are written as

$$w_i = \sum_{j \geq i} \alpha_{ij} x_i. \blacksquare$$

Summing up the proceeding claims, we have the following.

Lemma 2.27 *For any rigid PFTQ $\mathfrak{M} = \{M_0, \cdots, M_{g-1}\}$, there exists a standard basis Θ such that $\mathfrak{M} \in U^{\Theta}$.*

Lemma 2.28 *Let $\mathfrak{M} = \{M_0, \subset, M_{g-1}\}$ be a rigid PFTQ. If $\mathfrak{M} \in U^{\Theta}$, then M^i is generated by $\mathfrak{f}^i w_0, \mathfrak{f}^{i-1} w_1, \cdots, \mathfrak{f} w_{i-1}, w_i, w_{i+1}, \cdots, w_{g-1}$ as an $A_{\mathfrak{P}}$-module.*

Corollary 2.29 *For any rigid PFTQ $\mathfrak{M} = \{M_0 \subset \cdots \subset M_{g-1}\}$, we have a short exact sequence:*

$$0 \to M^{i-1}/M^i \xrightarrow{\mathfrak{f}} M^i/M^{i+1} \to R \to 0.$$

Proof. Since we have $M^i = M_0 \cap \mathfrak{f}^i M_{g-1}$, the injectivity of $\mathfrak{f}$ is clear.

By Lemma 2.27, there is a standard basis Θ such that $\mathfrak{M} \in U^{\Theta}$. From the above lemma, M^i/M^{i+1} is a free R-module generated by $\mathfrak{f}^i w_0, \mathfrak{f}^{i-1} w_1, \cdots, \mathfrak{f} w_{i-1}$ and w_i. Hence the cokernel of $M^{i-1}/M^i \xrightarrow{\mathfrak{f}} M^i/M^{i+1}$ is a free R-module of rank 1 generated by w_i. $\blacksquare$

Lemma 2.30 *U^{Θ} is an open subscheme of $\mathcal{N}_g$ and U^{Θ} depends only on $\Theta \bmod \mathfrak{p}$*

Proof. For a given $\Theta \in \tilde{\Phi}$, the condition $\{M_0 \subset M_1 \subset \cdots \subset M_{g-1}\} \in U^{\Theta}$ is equivalent to the property that the natural maps

$$\operatorname{coker}(M^{i-1}/M^{i} \xrightarrow{\mathfrak{f}} M^{i}/M^{i+1}) \to \mathfrak{f}^{i}M_{g-1}/\mathfrak{f}^{i+1}M_{g-1} \to R(x_i \bmod \mathfrak{p})$$

are surjective for all i. This is an open condition and depends only on x_i modulo $\mathfrak{p}$. ∎

We denote $\tilde{\Phi}$ modulo π by Φ. Then $\sharp\Phi$ is finite. In fact Φ is containd in the set of subsets with g elements of $\tilde{M}_{g-1} \otimes_{\mathcal{O}_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}}''/\pi(\tilde{M}_{g-1} \otimes_{\mathcal{O}_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}}'')$ which is finite.

The above lemma says that for $\Theta \in \Phi$, we have an open subscheme U^{Θ} of $\mathcal{N}_g$.

Proposition 2.31 $\coprod_{\Theta \in \Phi} U^{\Theta} \to \mathcal{N}^{g}$ *is a finite open covering.*

Let $\mathfrak{U}_m^{\Theta}$ be the category of pairs of filtrations of Dieudonné $\mathcal{O}_{\mathfrak{P}}$-modules

$$\{M_0' \subset \cdots \subset M_{g-3}'; M_m \subset \cdots \subset M_{g-1}\} \tag{26}$$

such that

(a) $\{M_0' \subset \cdots \subset M_{g-3}'\}$ is a rigid PFTQ and M_0' has generators $\{w_i'\}$ as in (25),

(b) $\{M_m \subset \cdots \subset M_{g-1}\}$ is a filtration of quasi-polarized Dieudonné $\mathcal{O}_{\mathfrak{P}}$-modules such that

  (b1) M_{g-1} is superspecial,

  (b2) $IM_i \subset M_{i-1}$ $\quad (m < i < g)$ and M_i/M_{i-1} is a locally free R-module of rank i,

  (b3) $I^iM_i \subset M^i := M_i^t$ $\quad (m \le i < g)$,

  (b4) $M_i = M_m + \mathfrak{f}^{g-1-i}M_{g-1}$ $\quad (m < i < g)$,

(c) there is a surjection $M_m \to A_{\mathfrak{P}}x$ and an isomorphism

$$M_{i-1}' \simeq M_i \cap M/A_{\mathfrak{P}}\mathfrak{f}^{g-1-i}y \quad (\max(m,1) \le i \le g-2) \tag{27}$$

compatible with the filtrations where M is the submodule generated by $x_1, \ldots, x_{g-2}, y$ in M_{g-1},

(d) $IM_i \cap M/A_{\mathfrak{P}}\mathfrak{f}^{g-i}y \subset M_{i-2}'$ $\quad (\max(m,2) \le i \le g-2)$ under the isomorphism (27).

For the natural truncation map $t_m : \mathfrak{U}_{m-1}^{\Theta} \to \mathfrak{U}_m^{\Theta}$, we have the following.

Lemma 2.32 *Fix an element $v_m \in M_m$ with x-coefficient 1. There is a bijection from the set*

$$t_m^{-1}(\{M'_0 \subset \cdots \subset M'_{g-3}; M_m \subset \cdots \subset M_{g-1}\}) \tag{28}$$

to the set consisting of

$$v = v_m + \beta_{g-m}\mathfrak{f}^{g-m-1}x_{g-m} + \cdots + \beta_{g-2}\mathfrak{f}^{g-m-1}x_{g-2} + \beta\mathfrak{f}^{g-m-1}y \in M_m \tag{29}$$

modulo $\mathfrak{f}^{g-m}M_{g-1}$ satisfying the following (A) and (B).

- *(A)* $(\mathfrak{f} - \pi^{\frac{d}{2}})v \mod A_{\mathfrak{P}}y \in M'_{m-3}$ *and* $(\mathfrak{v} - \pi^{\frac{d}{2}})v \mod A_{\mathfrak{P}}y \in M'_{m-3}$ *only when $m \geq 3$,*
- *(B)* $\langle v, I^{m-1}v\rangle_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{P}}$.

(When $m = 1$, (29) means $v = v_1 + \beta\mathfrak{f}^{g-2}y \in M_1$.)

Lemma 2.33 *Assume $m \geq 3$. Under the notations of the above lemma, (A) and (B) is equivalent to (A) and (B′) $\langle v, \pi^{\frac{d}{2}(m-1)}v\rangle_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{P}}$.*

Remark 2.34 *When $*$ is trivial, the very similar argument shows that (A) and (B) is equivalent to (A) and (B') $\langle x, \pi^{\frac{d}{2}(m-2)}\mathfrak{f}v\rangle_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{P}}$.*

Let $v_m = x + \zeta y + \sum \zeta_i x_i$ be as in Lemma 2.32. We can find $\mu_{g-m}, \cdots, \mu_{g-2}$ such that by choosing $\lambda_1, \cdots, \lambda_{g-m-1}, \lambda'_1, \cdots, \lambda'_{g-m-1} \in A_{\mathfrak{P}}$, we obtain

$$\begin{cases} (\mathfrak{f} - \pi^{\frac{d}{2}})v_m \ (\mathrm{mod}\ A_{\mathfrak{P}}y) - \sum\limits_{j<g-m} \lambda_j v'_j &= \sum\limits_{j \geq g-m} \mu_j \mathfrak{f}^{g-m}x_j, \\ (\pi^{\frac{d}{2}} - \mathfrak{v})v_m \ (\mathrm{mod}\ A_{\mathfrak{P}}y) - \sum\limits_{j<g-m} \lambda'_j v'_j &= \sum\limits_{j \geq g-m} \mu_j^{\sigma^{-1}} \mathfrak{f}^{g-m}x_j. \end{cases} \tag{30}$$

In fact, we can take μ_j and λ_j satisfying the first equation and $\lambda_j \in A_{\mathfrak{P}}\mathfrak{f}$. Multiplying $\pi^{-\frac{d}{2}}\mathfrak{v}$, we get the second equation.

Lemma 2.35 *When $m \geq 3$, (A) is equivalent to the following equations*

$$\begin{cases} \overline{\beta}_j^{\sigma} - \overline{\beta}_j &= \overline{\alpha}_{g-m,j}\overline{\tau} - \overline{\mu}_j, \\ \overline{\beta}_j - \overline{\beta}_j^{\sigma^{-1}} &= \overline{\alpha}_{g-m,j}\overline{\tau}' - \overline{\mu}_j^{\sigma^{-1}} \end{cases} \qquad (g - m \leq j \leq g-2) \tag{31}$$

with variables $\overline{\tau}$ and $\overline{\tau}'$, and (B′) is equivalent to the following equation. When $m < g-1$,

$$2\overline{\beta} = -2\sum_{1 \leq i < m} \overline{\zeta}_i \overline{\beta}_{g-1-i} - \overline{\varepsilon^{-1}\langle v_m, \pi^{\frac{d}{2}(m-1)}v_m\rangle_{\mathfrak{p}}} \tag{32}$$

and when $m = g - 1$, taking $v_{g-1} = x$,

$$2\overline{\beta} = - \sum_{i \leq g-2} \overline{\beta}_i \overline{\beta}_{g-1-i}. \tag{33}$$

In case of $m = 2$, there are two equations coming from

$$\langle v, \mathfrak{f}v \rangle_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{P}} \quad \textit{and} \quad \langle v, \pi^{\frac{d}{2}} v \rangle_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{P}}; \tag{34}$$

explicitly, when $g > 3$, we have two equations

$$\begin{cases} \overline{\beta} + \overline{\beta}^{\sigma} & = -\overline{\zeta}_1 \overline{\beta}^{\sigma}_{g-2} - \overline{\zeta}^{\sigma}_1 \overline{\beta}_{g-2} - \overline{\varepsilon^{-1} \langle v_2, \mathfrak{f}v_2 \rangle}_{\mathfrak{p}}, \\ 2\overline{\beta} & = -2\overline{\zeta}_1 \overline{\beta}_{g-2} - \overline{\varepsilon^{-1} \langle v_2, \pi^{\frac{d}{2}} v_2 \rangle}_{\mathfrak{p}}, \end{cases} \tag{35}$$

and when $g = 3$, taking $v_2 = x$, we get

$$\begin{cases} \overline{\beta} + \overline{\beta}^{\sigma} & = -\overline{\beta}_1 \overline{\beta}^{\sigma}_1, \\ 2\overline{\beta} & = -\overline{\beta}_1 \overline{\beta}_1. \end{cases} \tag{36}$$

When $m = 1$, we have

$$2\overline{\beta} = -\overline{\varepsilon^{-1} \langle v_1, v_1 \rangle}_{\mathfrak{p}}. \tag{37}$$

Remark 2.36 In the even case, different from the odd case, there are two equations in (A). Only when $*$ is non-trivial, we need the second equation for $m = 2$ in each case. Otherwise, the second equation for $m = 2$ is automatically satisfied, i.e., $\langle v, \pi^{\frac{d}{2}} v \rangle_{\mathfrak{p}} = 0$, because $\langle x, y \rangle_{\mathfrak{p}} = -\langle y, x \rangle_{\mathfrak{p}}$.

Lemma 2.37 *We have equalities as sets:*

$$\begin{aligned} M^i \cap A_{\mathfrak{P}} < x_i, x_{i+1}, \cdots, x_{g-1} > &= \mathcal{O}_{\mathfrak{P}}[\mathfrak{f}] < w_i, \cdots, w_{g-1} > \\ &= A_{\mathfrak{P}} < w_i, \cdots, w_{g-1} > . \end{aligned}$$

Proof. The first equality implies the second one, because the first term is an $A_{\mathfrak{P}}$-module. It is obvious that the first term contains the middle term. We shall prove the first term is contained in the middle term by induction. For $i = g - 1$, this is obvious. Assume that it holds for $i + 1$. Put $M(i) = A_{\mathfrak{P}} < x_i, x_{i+1}, \cdots, x_{g-1} >$. Since $M^i \cap M(i)/M^{i+1} \cap M(i) = R < \overline{w}_i >$, we get

$$M^i \cap M(i) = \mathcal{O}_{\mathfrak{P}} < w_i > + M^{i+1} \cap M(i).$$

Take element v of $M^i \cap M(i)$. Then $v = aw_i + m$ with $a \in \mathcal{O}_{\mathfrak{P}}$ and $m \in M^{i+1} \cap M(i)$. There is $b \in \mathcal{O}_{\mathfrak{P}}\mathfrak{f}$ such that $m = bw_i + m'$ with $m' \in M^{i+1} \cap M(i + 1)$. By the hypothesis of induction, we have $m' \in \mathcal{O}_{\mathfrak{P}}[\mathfrak{f}] < w_{i+1}, \cdots, w_{g-1} >$, which implies $v \in \mathcal{O}_{\mathfrak{P}}[\mathfrak{f}] < w_i, \cdots, w_{g-1} >$. ∎

Since we have $(\mathfrak{f}-\pi^{\frac{d}{2}})w_{i-1} \in M^i \cap A_{\mathfrak{P}} < x_i, \cdots, x_{g-1} >$, we can write as

$$(\mathfrak{f}-\pi^{\frac{d}{2}})w_{i-1} = \tau_{i,i}w_i + \tau_{i,i+1}w_{i+1} + \cdots + \tau_{i,g-1}w_{g-1}$$

for some $\tau_{i,j} \in \mathcal{O}_{\mathfrak{P}}[\mathfrak{f}]$. We note that $\overline{\tau}$ in Lemma 2.35 is equal to $\overline{\tau}_{1,g-m}$. Then we also have

$$(\pi^{\frac{d}{2}} - \mathfrak{v})w_{i-1} = \tau'_{i,i}w_i + \tau'_{i,i+1}w_{i+1} + \cdots + \tau'_{i,g-1}w_{g-1}$$

with $\overline{\tau'_{i,j}}^{\sigma} = \overline{\tau_{i,j}}$.

We can write w_i as

$$w_i = \mathfrak{f}^i x_i + \sum_{j>i}\sum_{k=i}^{j-1} \beta_{i,j}^{(k)} \mathfrak{f}^k x_j,$$

i.e., $\alpha_{i,j} = \sum_{k=i}^{j-1} \beta_{i,j}^{(k)} \mathfrak{f}^k$. Note that $\alpha_{i,j}$ make sense modulo $\mathfrak{f}^{i-j}A_{\mathfrak{P}}$ in the definition of U^{Θ}. We can choose $\beta_{i,j}^{(k)}$ such that $\beta_{i,j}^{(k)} \in \omega(R)$ for all $i+j < g-1$, with "Teichmüller lift" $\omega : R \to \mathcal{O}_{\mathfrak{P}}$ and

$$\langle w_i, w_{g-1-j}\rangle_{\mathfrak{p}} = \delta_{ij}\varepsilon.$$

Lemma 2.38 *We have $\overline{\tau}_{i,j} = \overline{\tau}_{g-j,g-i}$ if $*$ is trivial and $\overline{\tau}_{i,j} = -\overline{\tau}_{g-j,g-i}$ if $*$ is not trivial.*

Definition 2.39 *We define a set $\mathcal{J}$ consisting of maps $J : \{1, 2, \cdots, g-1\} \to \{0, 1, \cdots, \frac{d}{2}\}$ satisfying*

(1) $J(i) = J(g-i)$,

(2) $J(i) \leq \frac{d}{2} - J(i+1)$ for $i \leq [\frac{g-1}{2}]$,

and if $*$ is trivial

(3) $J(1) = \frac{d}{2} - J(2)$.

Definition 2.40 *For $J \in \mathcal{J}$, we define $t_{i,j}$ $(1 \leq i, j \leq g-1)$ in the following way:*

(0) $t_{i,j} = 0$ if $i > j$,

(1) $t_{i,i} = J(i)$ for all $i = 1, \cdots, g-1$,

(2) $t_{i,j} = \frac{d}{2} - J(i+1)$ for all $i < j < g-1-i$,

(3) $t_{i,g-1-i} = \frac{d}{2} - J(i)$ (resp. $\frac{d}{2}$) if $*$ is non-trivial (resp. trivial),

(4) $t_{i,g-i} = 0$,

(5) $t_{i,j} = t_{g-j,g-i}$.

Definition 2.41 *For* $J \in \mathcal{J}$, $\mathcal{N}_g^J$ *is the moduli space of rigid PFTQs* $\{M_0 \subset, \cdots, M_{g-1}\}$ *satisfying the image of the map*

$\mathfrak{f} - \pi^{\frac{d}{2}} : \mathrm{coker}(M^{i-2}/M^{i-1} \to M^{i-1}/M^i) \to \mathrm{coker}(M^{i-1}/M^i \to M^i/M^{i+1}) \simeq R$

is contained in $\pi^{\frac{d}{2}-J(i)}R$.

Definition 2.42 *We set*

$$d(J) := \sum_{i+j \leq g} t_{i,j}.$$

Proposition 2.43 *Let* J *be an element of* $\mathcal{J}$. $\mathcal{N}_g^J$ *is a smooth scheme of dimension* $d(J)$. *Choose an irreducible component* $\mathcal{N}_g^{J,irr}$ *of* $\mathcal{N}_g^J$ *and set*

$$\mathcal{N}_g' = \coprod_{J \in \mathcal{J}} \mathcal{N}_g^{J,irr}.$$

Then we obtain a quasi-finite surjective morphism

$$\mathcal{N}_g' \to D_g.$$

Proof. The dimension of $\mathcal{N}_g^J$ is the sum of the number of the parameters defining $\overline{\tau}_{i,j}$. Therefore it is suffices to show that $\mathrm{ord}_\pi \overline{\tau}_{i,j} \leq \frac{d}{2} - t_{i,j}$. By Lemma 2.35 and Definition 2.40, we can verify it. In order to show the last statement, we need more preparations, so we omit it. ∎

2.2 Coarse moduli spaces

Let $\mathcal{R}$ generally be a ring of finite type over $\mathbb{Z}$ with involution $*$. Let $\mathcal{A}_{g,d,N,\mathcal{R}}$ be the functor mapping locally noetherian scheme S to the set of abelian schemes X over S of dimension g with injective ring homomorphism $\mathcal{R} \to \mathrm{End}_S(X)$, $\mathcal{R}$-linear polarization of degree d^2 which Rosati involution induces $*$ on $\mathcal{R}$ and level structure $\sigma_1, \cdots, \sigma_{2g} : \mathbb{Z}/N\mathbb{Z} \to X[N]$, i.e., these are injective and the images generate $X_{\overline{s}}[N]$ at each geometric point $\overline{s} \in S$.

The functor $\mathcal{A}_{g,d,N,\mathcal{R}}$ has a coarse moduli scheme $A_{g,d,N,\mathcal{R}}$. Moreover if $N \geq 3$ it has a fine moduli space. This can be proved as in [17, Theorem 7.10, Appendix to Chapter 1,2].

We denote by $S_{g,d,N,\mathcal{R}}$ the supersingular locus of $A_{g,d,N,\mathcal{R}}$, i.e., the reduced closed subscheme of $A_{g,d,N,\mathcal{R}}$ whose closed points consist of supersingular points. Here we use the fact that supersingularity is a closed condition [13, Corollary 2.3.2].

Return to our situation, i.e., let $\mathcal{R}$ be $\mathcal{O}_L$ and the polarization principal. $\mathcal{S}_{n,L}$ denotes the coarse moduli space of principally polarized supersingular abelian varieties with endomorphism structure. From now on, we are going to investigate the moduli space over $\overline{\mathbb{F}}_p$.

The endomorphism structures on a superspecial abelian variety

$$\theta : L \to \mathrm{End}^0(E^n) \tag{38}$$

are all equivalent by the Skolem-Noether theorem. Since $\mathrm{End}(E^n)$ is a maximal order in $\mathrm{End}^0(E^n)$, $\theta : L \to \mathrm{End}^0(E^n)$ induces an inclusion $\mathcal{O}_L \to \mathrm{End}(E^n)$. From now on, we fix a θ. Let Λ be the finite set of equivalence classes of polarizations on a superspecial abelian variety with endomorphism structure L satisfying $e_\mathfrak{p} \ker \eta = E^\mathfrak{n}[\mathfrak{f}^{g_\mathfrak{p}-1}]$.

Let G be a flat finite commutative group scheme over a scheme S. We say G is an α-group, if the relative Frobenius and the relative Verschiebung vanish on G. This is equivalent to that G is locally a product of α_p ([15], p.339). An $(\alpha, \mathcal{O}_\mathfrak{p})$-group is an α-group with $\mathcal{O}_\mathfrak{p}$-action of which Dieudonné $\mathcal{O}_\mathfrak{P}$-module corresponding via Dieudonné functor is a finite R-free module. Here R is one defined in (22). We say that G has an $(\alpha, \mathcal{O}_\mathfrak{p})$-rank r, if the corresponding Dieudonné $\mathcal{O}_\mathfrak{P}$-module is of R-rank r.

Definition 2.44 Let η be an element of Λ. *A rigid PFTQ at* $\mathfrak{p}$ *over* S *with respect to* η consists of polarized abelian schemes (Y_i, θ, η_i) of dimension $\mathfrak{n}$ with endomorphism structure satisfying $Y_i = (Y_i)_\mathfrak{p}$ and $\mathcal{O}_L$-linear isogenies $\rho_i : Y_i \to Y_{i-1}$ $(0 < i < g_\mathfrak{p})$ satisfying $\rho_i^t \circ \eta_{i-1} \circ \rho_i$ $(0 < i < g_\mathfrak{p})$ such that

(i) $Y_{g_\mathfrak{p}-1} = E^\mathfrak{n} \times S$,

(ii) $\ker \rho_i$ is an $(\alpha, \mathcal{O}_\mathfrak{p})$-group of $(\alpha, \mathcal{O}_\mathfrak{p})$-rank i,

(iii) $\ker(Y_{g_\mathfrak{p}-1} \to Y_i) = \ker(Y_{g_\mathfrak{p}-1} \to Y_0) \cap Y_{g_\mathfrak{p}-1}[\mathfrak{f}^{g_\mathfrak{p}-1-i}]$ $(0 < i < g_\mathfrak{p})$,

(iv) $\eta_{g_\mathfrak{p}-1} = \eta \times S$,

(v) $\ker \eta_i \subset \ker \mathfrak{f}^{i-j}\mathfrak{v}^j$ $(0 \leq j \leq [i/2])$.

Proposition 2.45 *The category of rigid PFTQs at* $\mathfrak{p}$ *with respect to* η *has a fine moduli space* $\mathcal{P}_{g_\mathfrak{p},L,\eta}$, *which is a quasi-projective variety.*

Proof. In the same way as the proof of Lemma 3.7 in [16]. ∎

Lemma 2.46 $\mathcal{P}_{g_\mathfrak{p},L,\eta}$ *is isomorphic to* $\mathcal{N}_{g_\mathfrak{p}}$ *up to inseparable morphism.*

Proof. We can show this in a similar way as in [16, 7.4, 7.5]. ∎

Let $\mathcal{P}^{J,\mathrm{irr}}_{g_\mathfrak{p},L,\eta}$ and $\mathcal{P}'_{g_\mathfrak{p},L,\eta}$ be the schemes corresponding to $\mathcal{N}^{J,\mathrm{irr}}_{g_\mathfrak{p}}$ and $\mathcal{N}'_{g_\mathfrak{p}}$ respectively if $d_\mathfrak{p}$ is even. When $d_\mathfrak{p}$ is odd, we put $\mathcal{P}'_{g_\mathfrak{p},L,\eta} = \mathcal{P}_{g_\mathfrak{p},L,\eta}$. Finally we see that $\mathcal{S}_{n,L} \otimes \overline{\mathbb{F}}_p$ is realized by the quotient of the product of $\{\mathcal{P}'_{g_\mathfrak{p},L,\eta}\}_{\eta\in\Lambda}$:

Theorem 2.47 *Assume that p is odd only when there is* $\mathfrak{p}$ *such that* $d_{\mathfrak{p}}$ *is even. There exists a surjective and quasi-finite morphism*

$$\coprod_{\eta\in\Lambda}\prod_{\mathfrak{p}\in I_1\sqcup I_2}\mathcal{P}'_{g_{\mathfrak{p}},L,\eta}\to\mathcal{S}_{n,L}\otimes\overline{\mathbb{F}}_p. \tag{39}$$

Proof. The surjectivity and the quasi-finiteness follow from Proposition 2.43. ∎

The results of the preceding section imply the following.

Theorem 2.48 *Assume that p is odd only when* $d_{\mathfrak{p}}$ *is even.*

(1) When $d_{\mathfrak{p}}$ *is odd,* $\mathcal{P}'_{g_{\mathfrak{p}},L,\eta}$ *is irreducible and smooth, and we have*

$$\dim\mathcal{P}'_{g_{\mathfrak{p}},L,\eta}=d_{\mathfrak{p}}\left[\frac{g_{\mathfrak{p}}{}^2}{4}\right] \tag{40}$$

with $g_{\mathfrak{p}}=\mathfrak{n}/d_{\mathfrak{p}}$. *The generic point of* $\mathcal{P}'_{g_{\mathfrak{p}},L,\eta}$ *has a-number* 1.

(2) When $d_{\mathfrak{p}}$ *is even and* $*$ *(the action on* $L_{\mathfrak{p}}$ *in Definition 2.14) is non-trivial, we have*

$$\mathcal{P}'_{g_{\mathfrak{p}},L,\eta}=\coprod_{J\in\mathcal{J}}\mathcal{P}^{J,irr}_{g_{\mathfrak{p}},L,\eta}$$

and the dimension of $\mathcal{P}'^{J,irr}_{g_{\mathfrak{p}},L,\eta}$ *is* $d(J)$ *given in Definition 2.42 with* $g_{\mathfrak{p}}=2\mathfrak{n}/d_{\mathfrak{p}}$.

(2′) When $d_{\mathfrak{p}}$ *is even and* $*$ *is trivial, then* $g_{\mathfrak{p}}=2\mathfrak{n}/d_{\mathfrak{p}}$ *has to be even and we have*

$$\mathcal{P}'_{g_{\mathfrak{p}},L,\eta}=\coprod_{J\in\mathcal{J}}\mathcal{P}'^{J,irr}_{g_{\mathfrak{p}},L,\eta}$$

and the dimension $\mathcal{P}'^{J,irr}_{g_{\mathfrak{p}},L,\eta}$ *is* $d(J)$ *given in Definition 2.42*

2.3 Class numbers and mass formulas

In this section, we relate the number of the isomorphism classes of L-linear polarizations on (E^n,θ) with class numbers of unitary groups or quaternion unitary groups. By Theorem 2.47, we can see that the number of the irreducible components of our moduli space is equal to the class number mentioned above.

In this section, all schemes are supposed to be over $\overline{\mathbb{F}}_p$. Let E be a supersingular elliptic curve. Let E^n be a superspecial abelian variety with endomorphism structure

$$\theta:L\to\mathrm{End}^0(E^n). \tag{41}$$

Set $X=E^{n-1}\times 0+E^{n-2}\times 0\times E+\cdots+0\times E^{n-1}$. Then

$$\varphi_X:E^n\to(E^n)^t \tag{42}$$

is a principal polarization. Set $B = \mathrm{End}^0(E) \simeq \mathbb{Q}_{\infty,p}$ and $\mathcal{O}_B = \mathrm{End}(E)$, which is a maximal order of $\mathrm{End}^0(E)$. If we identify $\mathrm{End}^0(E^n)$ with $M_n(B)$, then the Rosati involution by φ_X is ${}^t\overline{(\ )}$ on $M_n(B)$.

Lemma 2.49 *If (E^n, θ) has an L-linear polarization $\eta = \varphi_{\mathcal{L}}$, then θ is equivalent to another endomorphism structure θ' satisfying*

$$\theta'(z^*) = {}^t\overline{\theta'(z)}. \tag{43}$$

Proof. By the definition of the L-linearity of the polarization,

$$\begin{aligned}\theta(z^*) =& \varphi_{\mathcal{L}}^{-1} \circ \theta(z)^t \circ \varphi_{\mathcal{L}} \\ =& (\varphi_X^{-1} \circ \varphi_{\mathcal{L}})^{-1} (\varphi_X^{-1} \circ \theta(z)^t \circ \varphi_X)(\varphi_X^{-1} \circ \varphi_{\mathcal{L}}) \\ =& (\varphi_X^{-1} \circ \varphi_{\mathcal{L}})^{-1}\, {}^t\overline{\theta(z)} (\varphi_X^{-1} \circ \varphi_{\mathcal{L}}).\end{aligned} \tag{44}$$

$g := {\varphi_X}^{-1} \circ \varphi_{\mathcal{L}} \in M_n(\mathcal{O}_B)$ satisfies $g = {}^t\overline{g} > 0$ [12, Proposition 2.8]. It is well-known that for such g, there exists $x \in GL_n(B)$ such that ${}^t\overline{x}x = g$. We can easily see that $x\theta(z^*)x^{-1} = {}^t\overline{(x\theta(z)x^{-1})}$. ∎

By this lemma, we can assume $\theta(z^*) = {}^t\overline{\theta(z)}$. F denotes the $*$-invariant subfield of L. Then F is a totally real number field. In fact, if F has a complex place v, putting $f = \theta(\sqrt{-1}) \in M_n(B_{\mathbb{R}})$ ($\sqrt{-1} \in F_v \simeq \mathbb{C}$), then $f = {}^t\overline{f}$ (since F is $*$-invariant). Hence, we have $-1 = f^t\overline{f} > 0$, which contradicts. If $*$ is non-trivial, L is a quadratic extension of F. There exists an element α of L such that $L = F(\alpha)$ and $\alpha^* = -\alpha$. Then $\alpha^2 = -\alpha\alpha^*$ is a negative element of F, so L has to be a totally imaginary quadratic extension of a totally real field, i.e., a CM-field. Hence we obtain

Lemma 2.50 *If there is an L-linear polarization on (E^n, θ), the field L has to be a totally real field or a CM-field. Moreover, $*$ is trivial (resp. non-trivial) if and only if L is a totally real field (resp. a CM-field).*

The centralizer of $\theta(L)$ in $M_n(B)$ is isomorphic to $M_m(D)$ where D is L (split case) or the division quaternion algebra $L \otimes_{\mathbb{Q}} B$ over L (non-split case) and

$$m = \begin{cases} \frac{2n}{[L:\mathbb{Q}]} & \text{if } D = L, \\ \frac{n}{[L:\mathbb{Q}]} & \text{if } D: \text{the division quaternion algebra over } L. \end{cases} \tag{45}$$

The involution ${}^t\overline{(\ )}$ on $M_n(B)$ induces that on $C_{M_n(B)}\theta(L)$, because we have ${}^t\overline{x}\theta(z) = {}^t\overline{(\theta(z^*)x)} = {}^t\overline{(x\theta(z^*))} = \theta(z)^t\overline{x}$ for any $x \in C_{M_n(B)}\theta(L)$ and for any $z \in L$. From now on, we assume that $*$ is trivial if D is a division quaternion algebra over L. This holds automatically if the extension $L/\mathbb{Q}$ is non-split at p. Then the involution on $M_m(D) \simeq C_{M_n(B)}\theta(L)$ induced by ${}^t\overline{(\ )}$ on $M_n(B)$ is equivalent to ${}^t\overline{(\ )}$ where the second $^-$ is the main involution on D over F

(resp. $*$) in case that D is a division quaternion algebra (resp. $D = L$). In fact, generally the involution on central simple algebra is uniquely determined up to equivalence by the involution on the center (Skolem-Noether's theorem). When D is a division quaternion algebra, the center D of $M_m(D)$ is identified to $L \otimes B \cdot 1_n$ in $M_n(B)$. Therefore the involution ${}^t\overline{(\ )}$ induces the main involution on the center D. Also in case that $D = L$, the same thing holds obviously.

For a prime ideal $\mathfrak{l}$ of F, we consider the set $\{f \in M_m(\mathcal{O}_{D_\mathfrak{l}}) | f = {}^t\overline{f}\}$. On this set, we define the local equivalence relation denoted by $\overset{\mathfrak{l}}{\approx}$:

$$f \overset{\mathfrak{l}}{\approx} f' \overset{\text{dfn}}{\Longleftrightarrow} {}^t\overline{g}fg = f',\ \exists g \in GL_m(\mathcal{O}_{D_\mathfrak{l}}). \tag{46}$$

Lemma 2.51 *Any $f \in M_m(\mathcal{O}_{D_\mathfrak{l}})$ satisfying $f = {}^t\overline{f}$ is locally equivalent to a representative f' given as follows:*

(1) if $D = L$,

(i) if L/F is inert or split at $\mathfrak{l}$, we can choose $f' = \mathrm{diag}(\mathfrak{l}^{r_i})$,

(ii) if L/F is ramified at $\mathfrak{l}$, we can choose

$$f' = \mathrm{diag}(\mathfrak{L}^{r_i}\varepsilon_i),\ \ \varepsilon_i \in \mathcal{O}_{F_\mathfrak{l}}^\times / N_{L_\mathfrak{L}/F_\mathfrak{l}}\mathcal{O}_{L_\mathfrak{L}}^\times$$

where $\mathfrak{L}$ is a place of L lying over $\mathfrak{l}$. Here r_i has to be even;

(2) if D is a quaternion algebra over $L = F$,

(i) if D is split at $\mathfrak{l}$, we can choose $f' = \mathrm{diag}(\mathfrak{l}^{r_i})$,

(ii) if D is non-split at $\mathfrak{l}$, we can choose $f' = \mathrm{diag}(A_i)$ with $A_i = \mathfrak{l}^{r_i}$ or $f' = \mathfrak{l}^{r_i}\begin{pmatrix} 0 & \mathfrak{f} \\ -\mathfrak{f} & 0 \end{pmatrix}$.

Let G be a finite subgroup in E^n satisfying

$$G \simeq G^D. \tag{47}$$

Let $\mathcal{E}_G$ be the set of local equivalence classes (i.e., for all $\mathfrak{l}$, locally isomorphic to $\varepsilon_\mathfrak{l}$) of $\varepsilon \in M_m(\mathcal{O}_D)$ such that $\varepsilon = {}^t\overline{\varepsilon} > 0$ and $\ker\varepsilon \simeq G$.

Remark 2.52 If L/F is unramified (in particular, $*$ is trivial), then $\mathcal{E}_G$ consists of one element for any G by the above lemma.

Lemma 2.53 *There exists a canonical bijection between the set of the L-linear isomorphism classes of polarizations η on (E^n, θ) satisfying $G = \ker\eta$ and*

$$\bigcup_{\varepsilon\in\mathcal{E}_G} \{f \in M_m(\mathcal{O}_D) | f = {}^t\overline{f} > 0, f \text{ is locally equivalent to } \varepsilon\}/\approx. \tag{48}$$

Here $\approx$ is a global equivalence relation, i.e., $f \approx f'$ means that there exists $g \in GL_m(\mathcal{O}_D)$ such that ${}^t\overline{g}fg = f'$.

Proof. The injection $\mathrm{NS}(E^n) \to \mathrm{End}(E^n)$ sending $\varphi_{\mathcal{L}}$ to $f_{\mathcal{L}} := \varphi_X^{-1} \circ \varphi_{\mathcal{L}}$ induces the map from

$$\{\text{polarization on } E^n \text{ with kernel } G\} \tag{49}$$

to

$$\{f \in M_n(\mathcal{O}_B) | f = {}^t\overline{f} > 0,\ \ker f \simeq G\}. \tag{50}$$

L-linearity of $\varphi_{\mathcal{L}}$ implies $\theta(z^*) = f_{\mathcal{L}}^{-1}{}^t\overline{\theta(z)} f_{\mathcal{L}}$. Now $\theta(z^*) = {}^t\overline{\theta(z)}$. Therefore $f_{\mathcal{L}} \in M_m(\mathcal{O}_D)$. Since $\varphi_{g^*\mathcal{L}} = g^t \circ \varphi_{\mathcal{L}} \circ g$ for $g \in \mathrm{Aut}_L(E^n) \simeq GL_m(\mathcal{O}_D)$,

$$\begin{aligned} \varphi_X^{-1} \circ \varphi_{g^*\mathcal{L}} =& \varphi_X^{-1} \circ g^t \circ \varphi_{\mathcal{L}} \circ g \\ =& (\varphi_X^{-1} \circ g^t \circ \varphi_X)(\varphi_X^{-1} \circ \varphi_{\mathcal{L}})g \\ =& {}^t\overline{g}(\varphi_X^{-1} \circ \varphi_{\mathcal{L}})g. \end{aligned} \tag{51}$$

Hence, we get the injection from

$$\{L\text{-linear polarization with kernel } G\} / \mathrm{Aut}_L(E^n) \tag{52}$$

to

$$\{f \in M_m(\mathcal{O}_D) | f = {}^t\overline{f} > 0\} / \approx . \tag{53}$$

Every element of the image is locally equivalent to a certain $\varepsilon \in \mathcal{E}_G$. This completes the proof. ∎

Let Π_G be the set of isomorphism classes of polarizations on (E^n, θ) with kernel G. Let $\Pi_{G,\varepsilon}$ be the subset of Π_G consisting of polarizations corresponding to f in the class ε. We identify $\Pi_{G,\varepsilon}$ with $\{f \in M_m(\mathcal{O}_D) | f = {}^t\overline{f} > 0, f \text{ is locally equivalent to } \varepsilon\}$ via the above lemma. Of course, $\Pi_G = \coprod_{\varepsilon \in \mathcal{E}_G} \Pi_{G,\varepsilon}$. For $\varepsilon \in \mathcal{E}_G$, we define algebraic groups G_ε and $\tilde{G}_\varepsilon$ over F by

$$G_\varepsilon(F) = \{g \in GL_m(D) | {}^t\overline{g}\varepsilon g = \lambda(g)\varepsilon,\ \lambda(g) \in F\} \tag{54}$$

and

$$\tilde{G}_\varepsilon(F) = \{g \in GL_m(D) | {}^t\overline{g}\varepsilon g = \varepsilon\}. \tag{55}$$

Let $\mathcal{L}_{G,\varepsilon}^{\mathrm{free}}$ be the set of free G_ε-lattices, i.e., $x\mathcal{O}_D^m$ for some $x \in GL_m(D)$ satisfying the local condition: for each finite place $\mathfrak{l}$ of F,

$$x_{\mathfrak{l}}\mathcal{O}_{D_{\mathfrak{l}}}^m = \gamma_{\mathfrak{l}}\mathcal{O}_{D_{\mathfrak{l}}}^m \tag{56}$$

with $\gamma_{\mathfrak{l}} \in G_\varepsilon(F_{\mathfrak{l}})$. We define a global equivalence relation on $\mathcal{L}_{G,\varepsilon}^{\mathrm{free}}$ by

$$x\mathcal{O}_D^m \sim x'\mathcal{O}_D^m \overset{\mathrm{dfn}}{\Longleftrightarrow} \exists g \in G_\varepsilon(F),\ x\mathcal{O}_D^m = gx'\mathcal{O}_D^m. \tag{57}$$

Proposition 2.54 *There exists a bijection*

$$\sim \backslash \mathcal{L}_{G,\varepsilon}^{free} \xrightarrow{\simeq} \Pi_{G,\varepsilon} \tag{58}$$

that sends $x\mathcal{O}_D^m$ *to* f *satisfying*

$$^t\overline{x}\varepsilon x = \lambda f \tag{59}$$

for some $\lambda \in F_+^\times$.

Proof. We begin with checking the well-definedness. Let $x\mathcal{O}_D^m$ be a free G_ε-lattice. By definition, $x_\mathfrak{l} = \gamma_\mathfrak{l}\delta$ for some $\gamma_\mathfrak{l} \in G_\varepsilon(F_\mathfrak{l})$ and $\delta \in GL_m(\mathcal{O}_{D_\mathfrak{l}})$. Putting $\lambda = \prod_\mathfrak{l} \lambda(\gamma_\mathfrak{l})$ and $f = \lambda^{-1}{}^t\overline{x}\varepsilon x$, we get $f \in \Pi_{G,\varepsilon}$. Let $x_1\mathcal{O}_D^m$ and $x_2\mathcal{O}_D^m$ be two elements of $\mathcal{L}_{G,\varepsilon}^{\text{free}}$. Suppose they are equivalent, i.e., there exists $g \in G_\varepsilon(F)$ such that

$$x_1\mathcal{O}_D^m = gx_2\mathcal{O}_D^m. \tag{60}$$

Let f_1 and f_2 be the corresponding elements of $M_m(\mathcal{O}_D)$, i.e., satisfying that ${}^t\overline{x_i}\varepsilon x_i = \lambda_i f_i$ for some λ_i as above. Then $\gamma := x_1^{-1}gx_2$ is in $GL_m(\mathcal{O}_D)$ by (60). The equation

$$\lambda_2\lambda(g)f_2 = \lambda(g){}^t\overline{x}_2\varepsilon x_2 = {}^t\overline{x}_2{}^t\overline{g}\varepsilon g x_2 = {}^t\overline{\gamma}{}^t\overline{x}_1\varepsilon x_1\gamma = \lambda_1{}^t\overline{\gamma}f_1\gamma \tag{61}$$

means that f_1 and f_2 are equivalent. Next, we see the injectivity. Let x_1, x_2, f_1 and f_2 be as above. Suppose f_1 and f_2 are equivalent, i.e., for some $\gamma \in GL_m(\mathcal{O}_D)$,

$$f_2 = {}^t\overline{\gamma}f_1\gamma. \tag{62}$$

Put $g := x_1\gamma x_2^{-1}$. It suffices to show $g \in G_\varepsilon(F)$, which follows from

$${}^t\overline{g}\varepsilon g = {}^t\overline{x_2}^{-1}{}^t\overline{\gamma}{}^t\overline{x}_1\varepsilon x_1\gamma x_2^{-1} = \lambda_1{}^t\overline{x_2}^{-1}{}^t\overline{\gamma}f_1\gamma x_2^{-1} = \lambda_1{}^t\overline{x_2}^{-1}f_2x_2^{-1} = \lambda_1\lambda_2\varepsilon. \tag{63}$$

We can verify the surjectivity in the following way. Let f be an element of the right side. Locally there exists $\delta \in GL_n(\mathcal{O}_\mathfrak{l})$ such that $f_\mathfrak{l} = {}^t\overline{\delta}\varepsilon_\mathfrak{l}\delta$. Then, there exists $x \in GL_m(D)$ such that

$${}^t\overline{x}\varepsilon x = f. \tag{64}$$

At any $\mathfrak{l}$,

$${}^t\overline{x}_\mathfrak{l}\varepsilon_\mathfrak{l}x_\mathfrak{l} = f_\mathfrak{l} = {}^t\overline{\delta}\varepsilon_\mathfrak{l}\delta. \tag{65}$$

This means that $\tilde{\gamma}_\mathfrak{l} = x_\mathfrak{l}\delta^{-1}$ is in $\tilde{G}_\varepsilon(F_\mathfrak{l}) \subset G_\varepsilon(F_\mathfrak{l})$. ∎

Corollary 2.55

$$\sharp\Pi_G = \sum_{\varepsilon\in\mathcal{E}_G} \sharp\left(\sim\backslash\mathcal{L}^{free}_{G,\varepsilon}\right). \tag{66}$$

Corollary 2.56 *If $M_m(D)$ is not a division quaternion algebra over F, we get the isomorphism*

$$\Pi_{G,\varepsilon} \simeq \tilde{G}_\varepsilon(F)\backslash\tilde{G}_\varepsilon(\mathbb{A}_{F,f})/\tilde{U}_\varepsilon \tag{67}$$

that sends f to $(\tilde{\gamma}_\mathfrak{l})_\mathfrak{l}$ in the proof of the above proposition. Here $\mathbb{A}_{F,f}$ is the finite adele ring and

$$\tilde{U}_\varepsilon = \prod_{\mathfrak{l}:\text{finite place}} \tilde{G}_\varepsilon(\mathcal{O}_{D_\mathfrak{l}}). \tag{68}$$

Proof. It suffices to show that $(\tilde{\gamma}_\mathfrak{l})_\mathfrak{l}$ in the right hand side defines a free G_ε-lattice. This follows from Eichler's theorem [3]. ∎

Remark 2.57 Let $\mathcal{L}_{G,\varepsilon}$ be the set of G_ε-lattices, i.e., lattices $\mathcal{O}$ in D^m satisfying that for all finite places $\mathfrak{l}$ of L,

$$\mathcal{O}_\mathfrak{l} = \gamma_\mathfrak{l}\mathcal{O}^m_{D_\mathfrak{l}} \tag{69}$$

with $\gamma_\mathfrak{l} \in G_\varepsilon(F_\mathfrak{l})$. Then attaching $\mathcal{O}$ to $(\gamma_\mathfrak{l})_\mathfrak{l}$, we get an isomorphism

$$\sim\backslash\mathcal{L}_{G,\varepsilon} \simeq G_\varepsilon(F)\backslash G_\varepsilon(\mathbb{A}_{F,f})/U_\varepsilon \tag{70}$$

with

$$U_\varepsilon = \prod_{\mathfrak{l}:\text{finite place}} G_\varepsilon(\mathcal{O}_{D_\mathfrak{l}}). \tag{71}$$

If the class number of $M_m(D)$ is 1, then $\mathcal{L}^{\text{free}}_{G,\varepsilon} = \mathcal{L}_{G,\varepsilon}$.

Example 2.58 If $L = \mathbb{Q}$, then for any G, $\mathcal{E}_G$ consists of one elements. The number of elements of

$$\sim\backslash\mathcal{L}^{\text{free}}_{G,\varepsilon} = \sim\backslash\mathcal{L}_{G,\varepsilon} \simeq G_\varepsilon(\mathbb{Q})\backslash G_\varepsilon(\mathbb{A}_f)/U_\varepsilon \tag{72}$$

is $H_n(p,1)$ (resp. $H_n(1,p)$) [12, p.140] if ε_p is 1_n (resp.

$$\begin{pmatrix} & \mathfrak{f} & & & & \\ -\mathfrak{f} & & & & & \\ & & & \mathfrak{f} & & \\ & & -\mathfrak{f} & & & \\ & & & & \ddots & \\ & & & & & \mathfrak{f} \\ & & & & -\mathfrak{f} & \end{pmatrix}). \tag{73}$$

Lemma 2.59 *Let η be an L-linear polarization, ε the element of $\mathcal{E}_{\ker \eta}$ associated to η, and $x \in GL_m(D)$, $g_\eta := (\tilde{\gamma}_\mathfrak{l})_\mathfrak{l} \in \tilde{G}_\varepsilon(F)\backslash\tilde{G}_\varepsilon(\mathbb{A}_{F,f})/\tilde{U}_\varepsilon$ as above. There is a canonical isomorphism*

$$\mathrm{Aut}_L(E^n, \eta) \simeq g_\eta \tilde{U}_\varepsilon g_\eta{}^{-1} \cap \tilde{G}_\varepsilon(F) \tag{74}$$

that maps g to xgx^{-1}.

By Corollary 2.56 and Lemma 2.59 the sum

$$\sum_{\eta \in \Pi_{G,\varepsilon}} \frac{1}{\sharp \mathrm{Aut}_L(E^n, \eta)}, \tag{75}$$

is equal to

$$\mathfrak{m}(\tilde{U}_\varepsilon) := \sum_{g_\eta \in \tilde{G}_\varepsilon(F)\backslash\tilde{G}_\varepsilon(\mathbb{A}_{F,f})/\tilde{U}_\varepsilon} \frac{1}{\sharp(g_\eta \tilde{U}_\varepsilon g_\eta^{-1} \cap \tilde{G}_\varepsilon(F))} \tag{76}$$

on the same assumption as in Corollary 2.56.

Recall a general formula of G. Prasad [25, Section 4]. Let G be an absolutely quasi-simple simply connected algebraic group over a totally real algebraic number field F. Assume that G_v is compact for any archmedian place v. Let $P = \prod_{\mathfrak{l}:\text{finite place}} P_\mathfrak{l}$ be a product of paraholic subgroups $P_\mathfrak{l}$. Then by G. Prasad's mass formula, we can calculate explicitly

$$\mathfrak{m}(P) := \sum_{g_i \in G(F)\backslash G(\mathbb{A}_{F,f})/P} \frac{1}{\sharp(g_i P g_i^{-1} \cap G(F))}. \tag{77}$$

On account of this mass formula, we have a good lower (and upper) bound of the class number:

$$\sharp Z(\tilde{G}_\varepsilon(F)) \cdot \mathfrak{m}(\tilde{U}_\varepsilon) \leq \sharp\left(\tilde{G}_\varepsilon(F)\backslash\tilde{G}_\varepsilon(\mathbb{A}_{F,f})/\tilde{U}_\varepsilon\right). \tag{78}$$

There are many examples of explicit calculations of mass formulas for $\varepsilon = 1$, see [8, Theorem 5.6] for $L = \mathbb{Q}$, [7, Proposition 9] in the case that D is a quaternion algebra over a totally real algebraic number field $L = F$. And there are a few examples of explicit calculations of class numbers, see [9, §1 p.29] in the case that L is an imaginary quadratic field remaining p, $m = 2$ and $\varepsilon = 1$, and [7, Part II, p.696] (resp. [6]) in the case that D is a quaternion algebra over $\mathbb{Q}$ and $m = 2$ (resp. $m = 3$).

References

[1] M. Demazure: *Lectures on p-divisible Groups.* Lecture Notes in Math. **302** (1972), Springer - Verlag.

[2] M. Demazure and P. Gabriel: *Groupes algébriques 1.* North Holland, Amsterdam (1970).

[3] M. Eichler: *Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren über algebraischen Zahlkörpern und ihre L-Reihen.* J. Reine Angew. Math. **179** (1938), pp.227-251.

[4] T. Ekedahl and F. Oort: *Connected subsets of a moduli space of abelian varieties.* Preliminary version of a preprint.

[5] G. van der Geer: *Cycles on the moduli space of abelian varieties* In: Moduli of curves and abelian varieties (The Dutch intercity seminar on moduli) (Eds. C. Faber and E. Looijenga), Asp. Math. E 33, Vieweg (1999), pp. 65-89.

[6] K. Hashimoto: *Class numbers of positive definite ternary quaternion hermitian forms.* Proc. Japan Acad. **59** (1983), pp.490-493.

[7] K. Hashimoto and T. Ibukiyama: *On class numbers of positive definite binary quaternion hermitian forms.* J. Fac. Sci. Univ. Tokyo **27** (1980), pp.549-601. Part II, ibid. **28** (1981), pp.695-699. Part III, ibid. **30** (1983), pp.393-401.

[8] K. Hashimoto and H. Koseki: *Class numbers of definite unimodular hermitian forms over the rings of imaginary quadratic fields.* Tôhoku Math. J. **41** (1989), pp.1-30.

[9] T. Hayashida: *A class number associated with the product of an elliptic curve with itself.* J. Math. Soc. Japan Vol. **20**, Nos.1-2, 1968.

[10] T. Ibukiyama: *On automorphism groups of positive definite binary quaternion hermitian lattices and new mass formula.* Advanced Studies in Pure Mathematics **15** (1989).

[11] T. Ibukiyama and T. Katsura: On the field of definition of superspecial polarized abelian varieties and type number. Compositio Math. **91** (1994), pp.37-46.

[12] T. Ibukiyama, T. Katsura and F. Oort: *Supersingular curves of genus two and class numbers.* Compositio Math. **57** (1986), pp.127-152.

[13] N. Katz: *Slope Filtration of F-Crystals.* Astérisque **63** (1979), pp.113-164.

[14] R. E. Kottwitz: *Points on some Shimura varieties over finite fields.* J. Amer. Math. Soc. 5, no. 2 (1992), pp.373-444.

[15] K.-Z. Li: *Classification of Supersingular Abelian Varieties.* Math. Ann. **283** (1989), pp.333-351.

[16] K.-Z. Li and F. Oort: *Moduli of Supersingular Abelian Varieties.* Lecture Notes in Math. **1680** (1998).

[17] D. Mumford, J. Fogarty and K. Kirwan: *Geometric Invariant Theory, Third Enlarged Edition.* Ergeb. Math. Grenzgeb. **34** (1994).

[18] P. Norman and F. Oort: *Moduli of abelian varieties.* Ann. Math. 112 (1980), pp.413-439.

[19] T. Oda: *The first de Rham cohomology group and Dieudonné modules.* Ann. Sci. École Norm. Sup. 4série, t.**2** (1969), pp.63-135.

[20] T. Oda and F. Oort: *Supersingular Abelian Varieties.* Intl. Symp. on Algebraic Geometry Kyoto (1978), pp.595-621.

[21] A. Ogus: *Supersingular K3 crystals.* Astérisque **64** (1979), pp.3-86.

[22] F. Oort: *Newton polygons and formal groups: Conjectures by Manin and Grothendieck.* Ann. of Math. **152** (2000), pp.183-206, Springer - Verlag.

[23] F. Oort: *A stratification of a moduli space of abelian varieties.* Progress in Mathematics, Vol. 195, (2001), pp.345-416, Birkhöuser Verlag Basel/ Switzerland.

[24] V. Platonov and A. Rapinchuk: *Algebraic Groups and Number Theory.* Pure and Applied Mathematics **139** (1994), Academic Press.

[25] G. Prasad: *Volumes of S-Arithmetic Quotients of Semi-simple Groups.* Publ. Math. Inst. HES **69** (1989), pp.91-117.

[26] J.-P. Serre: *Sur la topologie des variétés algébriques en caractéristique p.* Symposion Internacional de topologia algebraica (1958), pp.24-53.

[27] G. Shimura: *Some exact formulas on quaternion unitary groups.* J. Reine Angew. Math. **509** (1999), pp.67-102.

[28] J. Tate: *Endomorphisms of abelian varieties over finite fields.* Invent. Math. **2** (1966), pp.134-144.

[29] W. C. Waterhouse: *Abelian varieties over finite fields.* Ann. Sci. École Norm. Sup. 4serie **2** (1969), pp.521-560.